Feasibility Study and Conception of an Intelligent GSM Cell Phone Silencer

Jean-Marie Gorce, Anja Kléber, Fabrice Valois

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Feasibility Study and Conception of an Intelligent GSM Cell Phone Silencer

Jean-Marie Gorce, Anja Kléber, Fabrice Valois

N° 0268

September 2002

THÈME 1

Rapport technique

ISSN 0249-0803

Feasibility Study and Conception of an Intelligent GSM Cell Phone Silencer

Jean-Marie Gorce*, Anja Kléber†, Fabrice Valois‡

Thème 1 — Réseaux et systèmes
Projet ARÈS

Rapport technique n° 0268 — September 2002 — 76 pages

Abstract: The European regulatory authorities are about to change the laws that deal with the proscription of cell phone silencers, towards the acceptance of intelligent systems. This technical report describes a cell phone silencer concept based on the idea of changing the access control parameters on the channel BCCH and develops other intelligent methods, also based on changing parameters on the common downlink channels. Intelligent in the way that they hamper people from using their cellular phones in places where this is not desired, but let past emergency calls and calls originating from privileged phones. Also developed is a method that gives the network provider the control over all silencers within its network. This is done by smoothly integrating it in the Radio Resource Layer in a way that does not irritate other GSM devices, not taking advantage of this feature. The overall system can be applied to any regular cell phone.

Key-words: GSM network, silencer, signal processing

Ce travail a été financé par le contrat INSAVALOR n°008316

* Jean-Marie.Gorce@insa-lyon.fr
† anja.kleber@web.de
‡ Fabrice.Valois@insa-lyon.fr

Unité de recherche INRIA Rhône-Alpes
655, avenue de l'Europe, 38330 Montbonnot-St-Martin (France)
Téléphone : +33 4 76 61 52 00 — Télécopie +33 4 76 61 52 52

Etude et conception d'un brouilleur intelligent pour réseaux GSM

Résumé : Après le développement, ces dernières années, des téléphones mobiles auprès des utilisateurs, leur utilisation, parfois abusive dans des lieux communautaires tels que les cinémas, théâtres mais également prisons, tribunaux, ont poussé l'ART et le législateur a pubier en Juin 2001 une loi autorisant l'utilisation de brouilleurs de téléphones GSM. Aujourd'hui l'Europe suit la démarche française. L'exigence du texte de loi et de l'ART impose un certain nombre de contraintes sur ces brouilleurs parmis lesquelles : la possibilité de laisser passer les messages d'urgence et le respect du confinement. Ce rapport technique propose d'étudier la conception d'un brouilleur intelligent basé sur la modification des paramètres d'accès à une cellule GSM via la modification du canal BCCH. Nous passerons également en revue d'autres méthodes basées sur la modification d'autres canaux logiques communs sur le lien descendant. Nous proposerons également une extension à la norme GSM permettant au réseau de contrôler les brouilleurs via des modifications au niveau de la couche RR de GSM.

Mots-clés : Réseaux GSM, brouilleur intelligent, traitement du signal

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The history of European mobile telephony is based on a good many analogue mobile networks as in the beginning each country had its own standard. For France it was the Radiocom 2000, for West Germany and Austria the A-, B-, and finally the C-Netz, in the Nordic and Benelux countries it was the NMT 450, TACs in the UK and TRMI/TRMS for Italy. With the increasing internationalization of business and the demand for greater capacity, the need for a second generation of mobile networks became obvious . In 1982, telecom administrations of 26 European countries came together to the CEPT (Conférence des Administrations Européenes des Postes et Télécommunications) to discuss a French-German study about future development of mobile communications. As a result of this conference the Group Spécial Mobile (GSM) was founded with the aim to develop an integrative digital European mobile communication standard, supporting many millions of subscribers.

The switch to a digital network and the widespread usage of the same standard led to much smaller devices and an enormous reduction of costs. The cell phone has found its way into our everyday lives and nowadays is affordable for nearly everybody.

Unfortunately ethics for mobile phone usage have not grown at the same speed as the number of subscribers of mobile networks (see Figure 1.1).

Today, everyone claims his right to be obtainable anywhere and at any time. This means there are phones ringing in the middle of Beethoven's ninth or during an important political speech. If a phone rings in a cinema, a restaurant or a library this will not only disturb its owner but everyone around. Many other examples like concert halls, recording studios, religious places or boardrooms can be found and the well know signs (see Figure 1.2) attached to the walls do usually not result in the desired effect.

Besides the disturbing effect a ringing phone can have on the human environment, there are lots of other reasons the use of cell phones might not be appreciated. It is proved that in aeroplanes and hospitals cell phones can cause dangerous interference's with sensitive

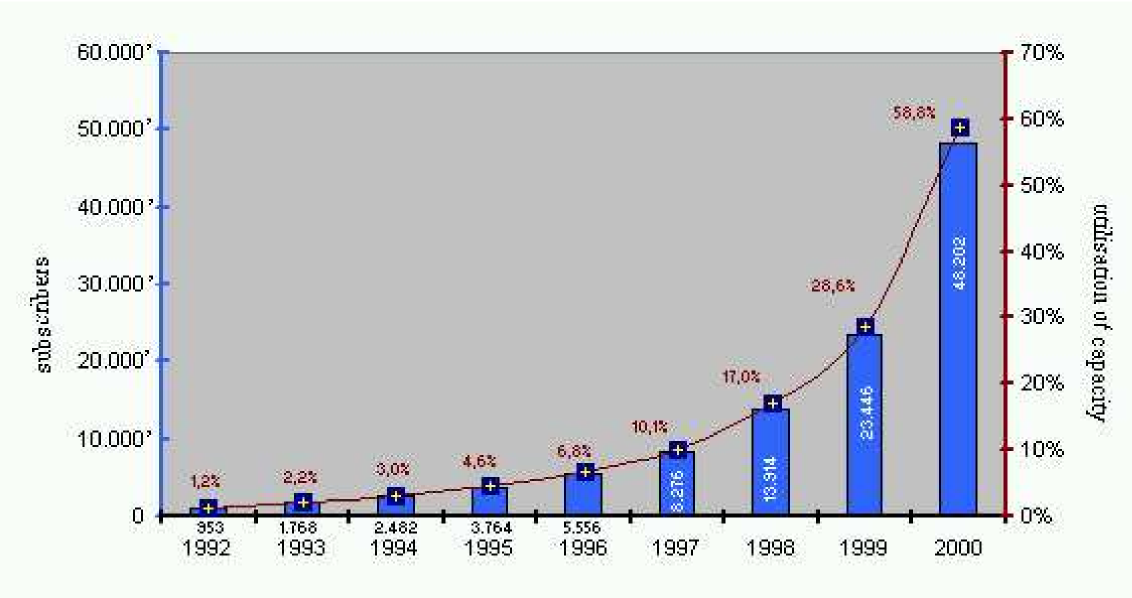

Figure 1.1: Subscriber development in Germany [RegTP '02].

Figure 1.2: Please turn off your mobile phone!

machines. Especially in these places it would be convenient to have the possibility to turn off cell phones automatically. Also for places like prisons where the misuse of mobile systems need to be abolished a so called cell phone silencer would be useful.

Cell phone silencer, mobile blocker, cellular disabler or jammer- there are various names for the possibility to oppress undesired mobile phone usage.

The simplest realization of this is a jammer device that transmits a random radio signal at the same frequency as the mobile phone. This cuts off the communication between the networks base station and the mobile device.

In the opera of Shanghai for example, such a jammer is installed statically and stops people from disturbing the performance. Cell phone silencers are also used in the US and in Japan where the law against cellular disabler was recently changed and now allows their usage in specially licensed places.

In Australia though they are prohibited by law. The government aims to protect their people from the electro-smog caused by constant emitting of random noise on the air interface. The Swiss regulatory authority for telecommunications and posts (BAKOM) simply reasons that jamming a certain frequency rebukes the idea of free telecommunication. The problem is firstly that it is nearly impossible to limit the sphere of action of the jammer device to a certain room (for the spreading feature of waves. This means that neighbors or passers-by are unwillingly affected, too. The cell phone silencer's antenna has to be placed reasonably and the emitting strength has to be balanced carefully. Secondly there is the fact that in most countries a regulatory authority sells the use of a certain frequency and guarantees at the same time that this frequency is not misused or disturbed by others. This is the main reason why the regulatory authorities of France (ART) [ART '02a] and Germany (Reg TP) [RegTP '02], too, put high penalties on the operation of a jammer device of the method described above. But recently a new discussion has arisen about different techniques for cellular disablers and how the law (for France see [ART '01]) might be changed for the more "intelligent" ones.

The ART classifies the different techniques as follows [ART '02b].

Type 1 device that constantly emits random noise to disturb the GSM/UMTS frequencies,

Type 2 device that starts emitting random noise on detection of a mobile in the zone that is to be protected,

Type 3 device that starts emitting random noise on detection of a communicating cellular phone in the zone that is to be protected,

Type 4 device that sends messages to a mobile phone to force it to switch to limited service,

Type 5 device that changes the BCCH, broadcasted by the closest base station, in a way that forces the cell phones to switch to limited service,

Type 6 device that detects communicating cell phones and notifies the network operation, asking for a filtration of the concerned communication.

Devices of type one to three, i.e. the rather non-intelligent types, exist in several versions and are sold and used in some countries but forbidden in most of them. A device of type 4 has been developed by the US-company Bluelinx in co-operation with the Australian university of Adelaide. Their "Q-Zone" [Bluelinx '02] system is based on Bluetooth-technology. Specially Bluetooth-equipped mobile phones switch to limited service or vibration alarm when entering a protected zone. The cell phone disabler is only about the size of a cigarette box. The disadvantage of this technique will probably be the acceptance on behalf of the customer.

In this technical report a concept of a device of type five will be compiled and other "intelligent" concepts will be presented and discussed.

The project has been realized in collaboration with M. Girod, the director of Altophone, who takes out a patent on intelligent cell phone silencers in 30 countries (see appendix) [Girod '02]. The application for these patents have been made in the 1990s, i.e. in the early stage of GSM.

For a better understanding of the methods of resolution an introduction to the concerned functions and parameters of the GSM standard will be given in chapter two. Chapter three introduces different concepts for intelligent cell phone silencers that have been found and/or developed during the research process. It also provides a range of possibilities for operation status control and itemizes available platforms and DSPs that can possibly serve as hardware for a mobile blocker concept. Chapter four presents and details the silencer concept, the operation status control concept and the platform that have been proved most suitable. Chapter five finally introduces to the SIMULATOR, the program that implements the ideas of chapter four and simulates the communication between a base station, a cell phone silencer and a mobile phone. As a rounding off chapter, chapter six introduces two other projects that are linked to this one.

Chapter 2

Overview GSM

2.1 Some General GSM concepts

2.1.1 The TDMA model

In older standards of mobile systems, like the C-Netz in Germany (450Hz), specific frequency for every user during a call (Frequency Division Multiple Access - FDMA) were allocated. Nowadays this would soon cause an overload problem. GSM uses an access scheme called Time Division Multiple Access (TDMA) with eight basic physical channels per carrier and a carrier separation of 200kHz. Every impulse on a certain frequency is called a burst, which corresponds to one of the eight time slots (TS). Altogether these TS form a TDMA frame with a duration of $\sim$4,62 sec. Every TDMA frame has a so called frame number (FN) which repeats itself every 3h, 28 min, 53 seconds and 760 milliseconds. This time period is referred to as hyperframe and it is needed to support cryptographic mechanisms. FN 2715647 hence is followed by FN 0. The hyperframe itself is divided into 2048 superframes which again are divided (for the common channels) into 26 51-multiframes. A 51-multiframe contains 51-TDMA-frames which refer, as already mentioned, to eight TS of a frequency (see figure 2.1). [Heine '98] [05.01 '99]

2.1.2 Physical and logical channels

As mentioned in section 2.1.1 the physical channels consist of all the available TS of a BTS (base transceiver station). Each TS of a certain frequency hence forms to one physical channel.

On the other hand there are logical channels which each perform a special task. There are twelve different types of logical channels in GSM. Distinctions should be made between

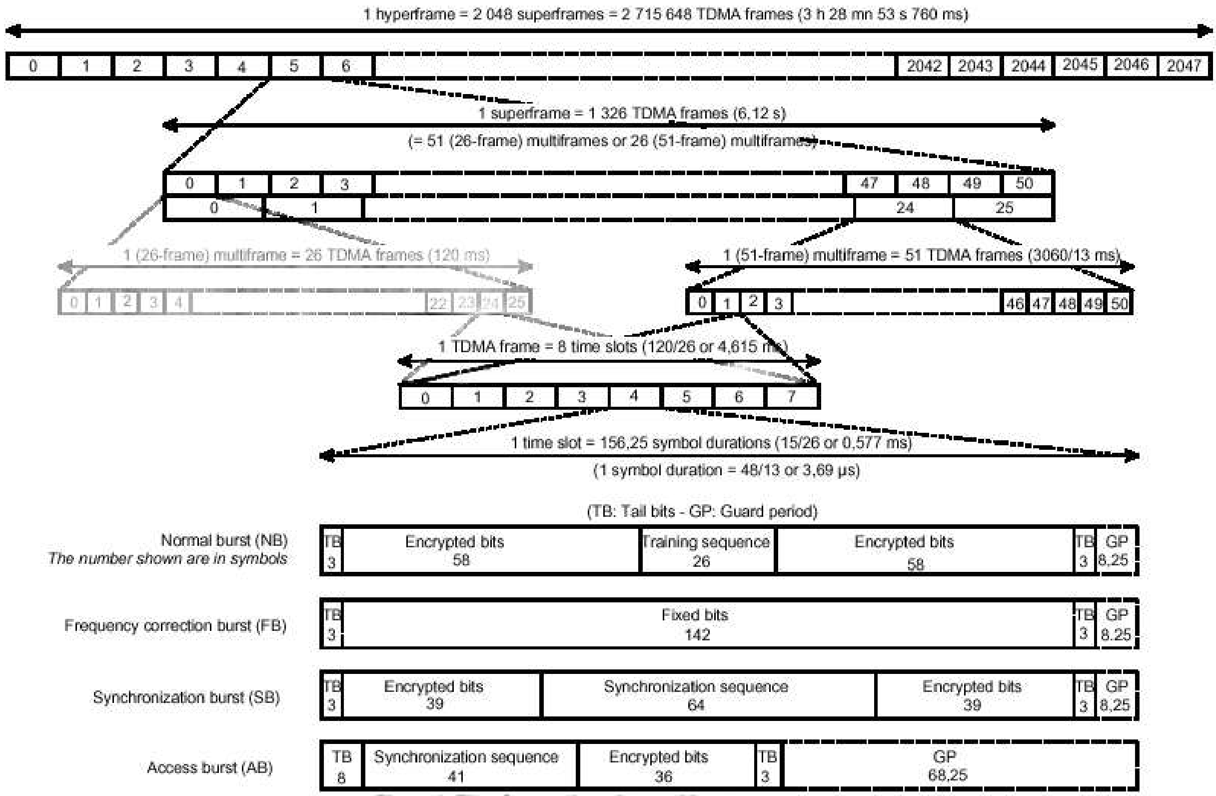

Figure 2.1: TDMA-frame hierarchy and bursts.

dedicated channels, which are dedicated to a specific user and common channels which are shared by all users. Dedicated Channels are duplex which means they need a pair of slots (downlink ↓ and uplink ↑) whereas common channels are simplex and only need one slot. Table 2.1 summarizes the logical channels and gives a short description of their tasks.

Each TS 'x' exists either 51 times in a 51-frame multiframe (common channels) or 26 times in a 26-mulitframe. The physical channel TS 'x' can hence be used 51 (or 26) times by a different logical channel.

Within this technical report only the common channels are regarded. That implicates that all concerned channels are simplex and transmitted via a 51-multitrame.

Generally speaking there are lots of different ways of mapping logical channels on a physical one. For the TS 0, the TS used for the common channels and therefor the most important

BCH ↓	Frequency Correction Channel (FCCH) Synchronization Channel (SCH) Broadcast Control Channel (BCCH)	repetition of the FBs FN and BSIC system information
CCCH ↑↓	Paging Control Channel (PCH) ↓ Random Access Channel (RACH) ↑ Access Grant Channel (AGCH) ↓ Cell Broadcast Channel (CBCH) ↓	call announcement cell phone random access resource allocation Short Message distribution
Dedicated Control Channel	Stand-Alone Ded. C. Ch. (SDCCH) Slow Associated C. Ch. (SACCH) Fast Association C. Ch. (FACCH)	signalling supervision of the link for handover use
TCH	Traffic for coded speech (TCH-FS/HS) Traffic Channel for data ($\leq$ 9,6 kbit)	Full/Half rate Speech Traffic user data

Table 2.1: Description of the logical channels.

for this report, there are two possible channel configurations, as specified in [05.02 '99], 6.5.1 and as folllows.

1. FCCH+SCH+BCCH+CCCH
2. FCCH+SCH+BCCH+CCCH+SDCCH/4(0...3)+SDCCH/C4(0...3)

A possible configuration of TS 0 is given in table 2.2.

In both configurations the FCCH is broadcast in FN 0, 10, 20, 30, 40, the SCH in FN 1, 11, 21, 31, 41 and the BCCH in FN 2 to 5.

2.1.3 Bursts

A time slot lasts 0,577ms. In this period 156,25 symbols can be transmitted on a *burst*. There are different bursts (see figure 2.1) specified for different logical channels.

Most channels transmit their data on a *normal burst*. A normal burst starts with three tail bits. Tail Bits are always set to *0* since in GSM the message *no information* is coded with *1*'s. The sending of a *0* announces hence the beginning of data transmission. The tail bits are followed by the encrypted data. The subsequent training sequence used for GMSK modulation (Gaussian pre-filtered minimum shift keying) is defined as shown in appendix 7 (see [05.04 '99]). The normal burst ends with another three tail bits that follow the second part of the encrypted data bits and a guard period. The guard period contains

FN	TS 0
0	FCCH
1	SCH
2-5	BCCH
6-9	AGCH/PCH
10	FCCH
11	SCH
12-19	AGCH/PCH
20	FCCH
21	SCH
22-25	SDCCH 0
26-29	SDCCH 1
30	FCCH
31	SCH
32-35	CBCH
36-39	SDCCH3
40	FCCH
41	SCH
42-45	SACCH 0
46-49	SACCH 1
50	idle

Table 2.2: Possible configuration for TS 0.

no information (bits) and serves as separator between two bursts. The output power during the guard period is lower than the power during the useful part of the burst.

The *frequency burst* is sent on the logical channel FCCH. It starts with three tail bits, followed by 142 fixed bits and another three tail bits. All these bits are set to *0*. The FB ends with a guard period of 8,25 bits.

The *synchronization burst* is used to broadcast messages on the SCH. The actual encrypted message bits are surrounded by the tail bits and the burst ends with a guard period as usual. Bit 42-105 represent an extended training sequence and divides the encrypted bit sequence in two parts. The training sequence is also given in appendix 7.

The *access burst* is sent on the AGCH. It is led by seven extended tail bits as given in appendix 7, followed by 41 synchronization bits that are also given in the appendix. The actual encrypted message bits are followed by three tail bits and the guard period.

2.1.4 The GSM network model

Similar to the ISO/OSI reference model all data transactions within the GSM specification are ordered in several layers. Different layer models exist for each of the GSM components MS, BTS, BSC and MSC. The layers of the MS and the BTS are as shown in figure 2.2.

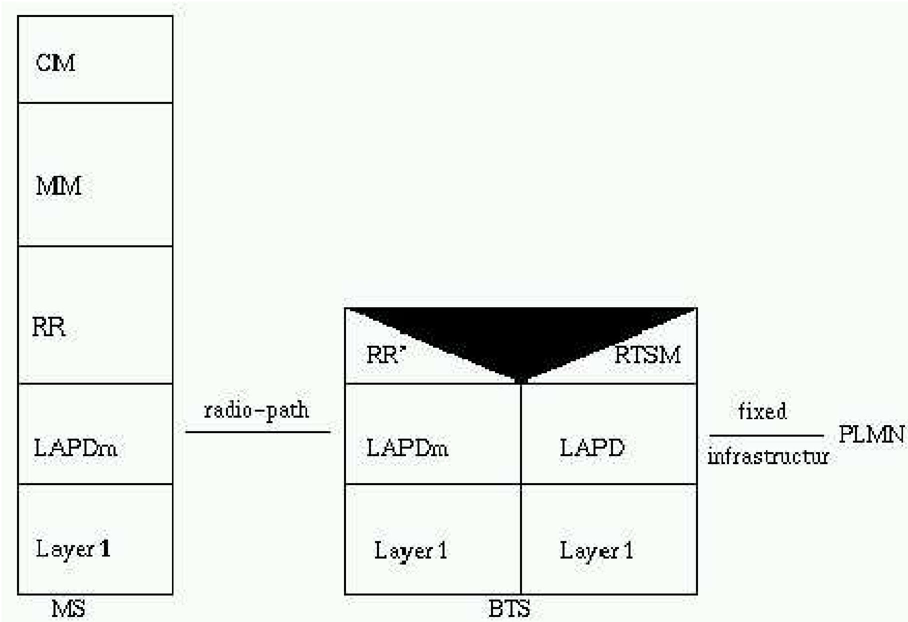

Figure 2.2: The GSM network model.

- The Communication Management (CM) layer provides call control, supplementary services management, and the short message services (SMS).
- The Mobility Management (MM) layer maintains the location data and provides authentication and ciphering procedures to ensure user identification confidentiality.
- The Radio Resource (RR) procedures control physical channels and data link connections on control channels. Their general purpose is to establish, maintain and release point-to-point connections between the MS and the network including cell selection and handover.
- The RR' layer is the corresponding layer managed by the BTS.
- As a data link layer protocol the (ISDN) LAPD protocol (Link Access Protocol for the ISDN D-channel) is in charge of providing error-free transmission (here: between the BTS and BSC).
- The layer two protocol on the MS side is the LAPDm air-interface protocol. This protocol is a modified version of the LAPD protocol, "m" stands for mobile.

- The Base Transceiver Station Management (BTSM) takes over the functionalities of the RR procedures on the BTS-BSC connection.

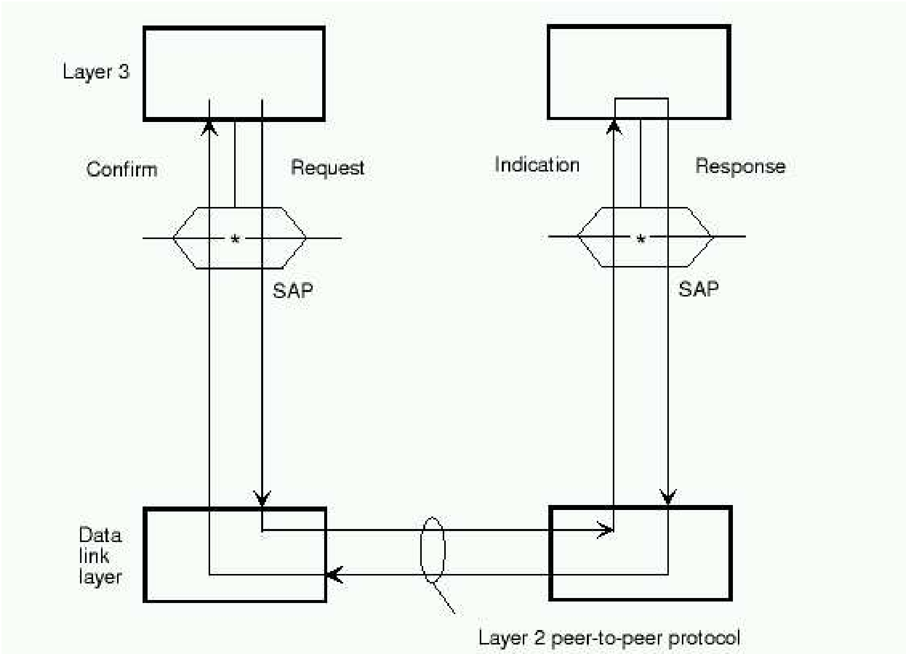

Figure 2.3: Communication between layer 3 and the data link layer.

Layers communicate using "Request/Confirm" or "Indication/Response"-pairs (see figure 2.3). Functions of the (N+1)th-layer can only be performed if a N-layer connection has been established. The establishment of these connections is to be triggered by the (N+1)th-layer. [04.08 '98] 4.1, 7.3 [04.06 '99] 4.1

A cell phone silencer, that in based on the idea of changing parameters of the BCCH, works on the Radio Resource Management level.

2.2 GSM Functions

2.2.1 Choosing a cell

When a mobile system is switched on, it changes from MM-NULL status (power off) to the initial status of the MM, the MM-IDLE (NORMAL SERVICE) status and starts a "cell selection procedure".

Generally there are two different possibilities of choosing a cell. See figure 2.4.

- If the MS does not have any knowledge of which RF channels are BCCH it searches for the strongest 30 (GSM 900) or 40 (DCS 1800) RF channels to find out which of them are BCCH and belong to the appropriate PLMN. The MS does not always need to search all 30 or 40 channels since a list of RF channels containing BCCH carriers is broadcast by the PLMN or can coded on the SIM card.
- Optionally the MS can store a list of RF channels that do fulfil these restraints when it is switched off. The subsequent time it is turned on it can reuse the so called BA(BCCH) list.

[03.22 '99] 3.2, 4.8

It then checks the cell list in descending order of receiving signal strength for a suitable cell to camp on. "Suitable" means that the cell is in the selected PLMN, not totally barred by the provider, not in a forbidden LA etc. Usually the MS will find such a cell and stay in MM-IDLE (NORMAL SERVICE).

To inform the network about its presence and the cell it has chosen, the mobile initiates a "location update" as described in section 2.2.2.

Once the mobile has chosen its cell it will steadily listen to

- the BCCH, to receive system information,
- the PCH, to survey eventual call announcements broadcast by the system.

2.2.1.1 Abnormal case: Limited Service

If general service access to the chosen cell is not granted for a mobile, i.e. the RACH Control Parameters (see section 2.3.3) broadcasted by the cell indicate a denial of any service apart from emergency calls to the MS, the MS will ignore this information and camp on it as well.

"... it shall not reject a cell for camping on because access on that cell is not allowed."[04.08 '98] 3.5.3

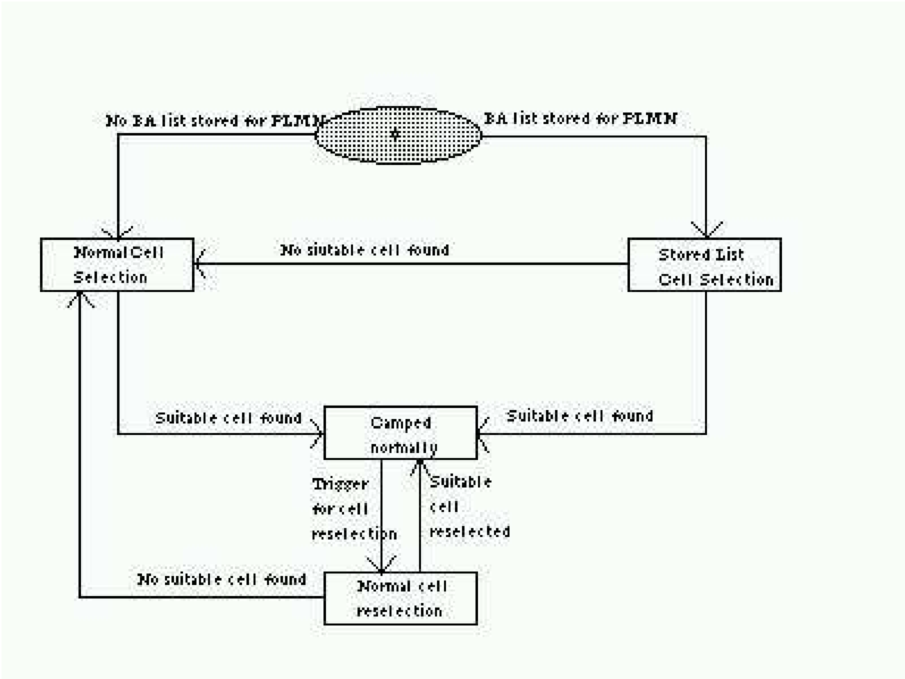

Figure 2.4: Cell selection state diagram.

In this case though the MM, which still is in MM-IDLE (NORMAL SERVICE) mode, will change to MM-IDLE (LIMITED SERVICE) status. LIMITED SERVICE status means that a cell is selected which is not known to provide normal service and which only offers emergency services.

In this mode the MS does

- "not perform any periodic updating",
- "not perform IMSI detach",
- "reject any request from CM entities for MM connections except for emergency calls,
- "perform normal location updating when a cell is entered which may perform normal services",
- "not respond to paging",

[04.08 '98] 4.2

From this it follows that no "normal" calls and no text messages can be sent or received in this mode. However, normal cell reselection will still be performed if the barred state is ended or if the MS chooses a new cell with a bigger signal strength. [04.08 '98] 4.4.4.9

2.2.2 Location updates

In GSM a location area system is implemented which allows the network to keep track of the position of its subscriber MS. Therefor the network base stations are grouped in so called localization areas (LA) consisting of one or more cells. The MS is in charge of informing the network of its current LA using the *location update procedure* visualized in figure 2.5.

There are three main mechanisms to update the mobiles position [04.08 '98].

Normal location updating Each LA has an LA Identifier (LAI) that is regularly broadcasted over the LAs cells BCCHs to notify the MS of the LA it is located in. If the MS observes a change of LAI it informs the network which can hence update the LA-properties saved for this mobile.

Periodic updating is an additional tool to keep the network periodically informed about the location of a mobile. It shows to the network that the mobile has not been switched off without notification of the network. The mobile initiates the normal location update procedure whenever the timer 3212 expires. The maximum value of this timer is broadcast on the BCCH in the System Information Type 3's Control Channel Description information element (see appendix 7). Its values can range between 6 minutes and 25,5 hours. If the value on the BCCH is set to 0 no periodic updating is expected. The timer is re-initialized on every interaction with the network.

If, in LIMITED SERVICE, the timer expires, the mobile delays the location update procedure until normal service is provided.

ISMI attach is executed if the mobile is switched on, a SIM card is inserted and IMSI attach is wanted by the network (ATT flag in System Information Message Type 3). The IMSI attach procedure uses the location update procedure.

[04.08 '98]4.4

2.2.3 Making and receiving calls

Once camped on a cell the mobile can start using services offered by the network.

The general concept of receiving calls in GSM is as follows. If a mobile is called the network will send a paging message on the PCH (part of the CCCH). The mobile always monitors this channel and on observation of a paging message addressed to its IMSI, it will answer the network on the RACH. The answer includes a request for a dedicated channel (in this case a TCH) on which circuit switched services can be used. This request can also be initiated by the mobile subscriber itself, i.e. if he wants to make a call. In both cases the network tries to reserve a dedicated channel for the MS. No other entity will use this channel while it is assigned to this mobile. Assignment information will be sent on the AGCH. The assignment ends with either abortion on behalf of the network, of the mobile or of the mobiles communication partner. Details of these procedures are given in section 2.3.4, 2.3.5 and 2.3.6.

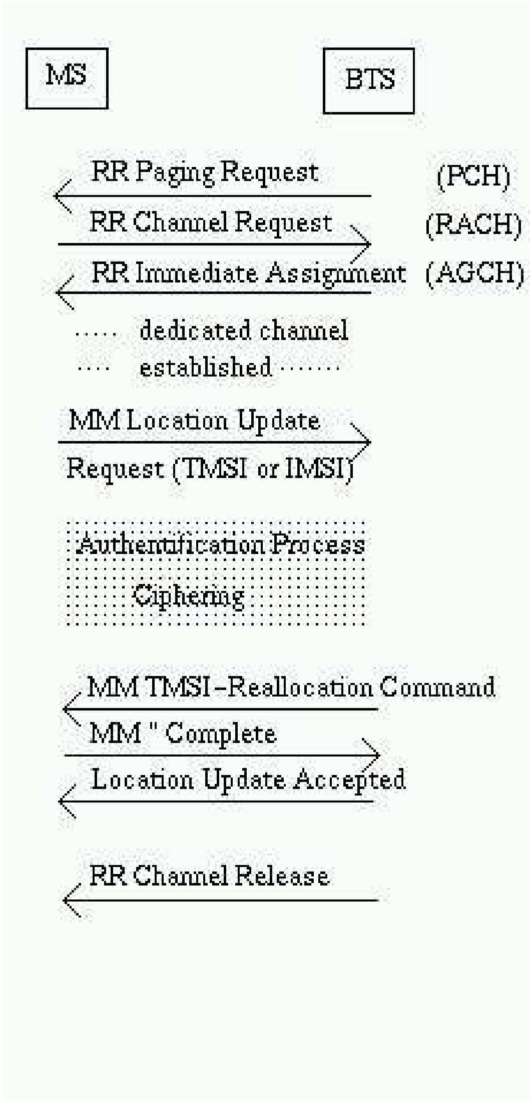

Figure 2.5: Messages sent during a location update procedure.

2.2.4 Sending and receiving text messages

The procedure for sending or receiving text messages (SMS) is similar to the procedure for making or receiving calls.

If a text message is sent to a mobile the network will send a paging message on the PCH, indicating that it only needs to demand for a SDCCH. The mobile subsequently sends a paging answer on the RACH including the request for such a dedicated channel. The network then informs the mobile about the properties of the assigned channel and sends the text message on this channel.

If it is the mobile subscriber sending a text message the procedure is exactly the same except for that the channel request on the RACH is not a paging answer but a simple dedicated channel request for sending non-voice data. For more details of these procedures see also sections 2.3.4, 2.3.5 and 2.3.6.

2.3 A closer view on certain channels

2.3.1 The Frequency Correction Channel

The FCH is one of the channels of the BCH. It is only required for the operation of the radio subsystem and its only task is to carry information for frequency correction of the MS. It has no supplementary information about the BTS or the network. The FCCH hence provides only information about the existence of a cell using the concerned frequency which enables the MS to measure the signal strength. The so called Frequency Burst (FB) is directly mapped on the TS0 (see figure 2.1 and table 2.1), there is no coding or the like, since there is no bit-information to be broadcasted. [05.02 '99] 3.3.2

2.3.2 The Synchronization Channel

The SCH aims to help the mobile to synchronize to a BTS. It provides a long training sequence for synchronization and the Frame Synchronization Element, consisting of the following data (see figure 2.6):

- The 6-bit BSIC, composed of 3 bits for the NCC (PLMN Colour Code) and 3 bits for the BCC (BTS Colour Code), which uniquely identifies a BTS,
- the 19-bit RFN (Reduced TDMA-Frame Number).

The BSICs purpose is to avoid ambiguity or interference that can arise when an MS in a given position can receive two cells using the same BCCH frequency. It also influences the access bursts sent by the MS and impedes one cell from directly decoding access bursts sent to another cell. Furthermore the BCC indicates the type of training sequence (see appendix) used in the bursts sent on the download common channel of the cell.

(It has, on the other hand, nothing to do with the cell identity broadcast on the BCCH. When the MS is in idle mode, the MS selects a cell according to the cell identity- not by the BSIC.)

The RFN contains the three parameters

- T1 $(0 \ldots 2047) =$ FN div $(26 * 51)$,
- T2 $(0 \ldots 25)=$ FN mod 26,
- T3' $(0 \ldots 4)=$ (T3-1) div 10, whereat T3 $(0 \ldots 50)=$ FN mod 51.

[04.08 '98] 9.1.30 [05.02 '99] 3.3.2.2.1

The FN can be calculated from the RFN as follows.

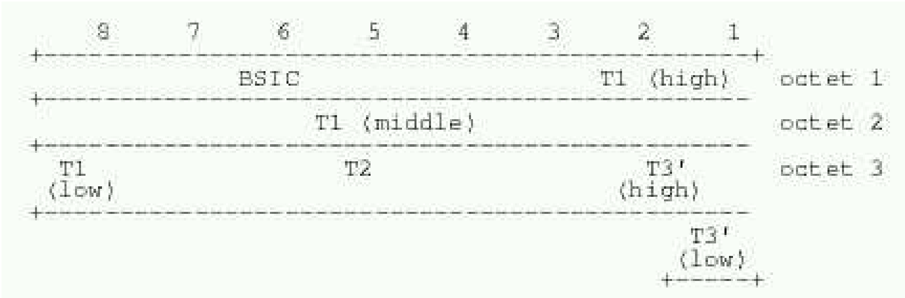

Figure 2.6: The Frame Synchronization Information Element.

FN= 51 $*$ ((T3-T2)mod 26)+ T3 +51$*$26$*$T1 where T3= 10$*$T3'+1.0

[05.10 '99] 4

The Synchronization Information Element consists hence of 25 Bits. These Bits are correction coded as described in 2.4.1 resulting in a 77 bit message which is split up into 2 39-bit sections emitted in a synchronization burst as shown in figure 2.1.

2.3.3 The Broadcast Control Channel

In idle mode the mobile listens to the BCCH, which is intended to broadcast regularly all necessary information to the MS which it needs to register in the system. The network will provide the following information:

- identification of the network, location area and cell,
- information for candidate cell measurement,
- description of the control channel structure,
- utilization of the RACH,
- different supported options,
- length of the message part belonging to phase 1 protocol,
- BCCH scheduling (optional).

This data will be delivered in System Information Messages.

Every System Information Message is wrapped into a 23-byte-word. After these 23 bytes are (correction) coded and interleaved (see section 2.4.2). The word, now extended to 456 bits plus 4$*$2 flag bits, is sent on the four bursts of every multiframe reserved for the BCCH (see table 2.1). This means there is one System Information Message transmitted every 235,38 ms.

There are eleven different types of System Information Messages reserved for BCCH usage. Some of them are optional, some mandatory. Mandatory are messages of type 1-4,7 and 8, optional are messages of type 2bis, 2ter,9,16 and 17. The last three optional messages are sent if indicated in System Information Message Type 3. All System Information Messages that can possibly be sent on the BCCH are listed in 7

Besides general information, as already mentioned above, some Message Types contain information about access permission to the network. All members with an inserted SIM are members of one out of 10 access classes numbered 0...9. In addition, mobile stations may be members of one or more out of 5 special access classes (11...15).The access class number(s) are stored in the SIM. Certain System Information Messages broadcast a list of authorized classes and authorized special access classes, and whether and to whom emergency calls are allowed. If the establishment cause is 'emergency call', access will either be allowed to any mobile in the cell or only to those that are members of at least one authorized special class, depending on the configuration of the so called *RACH Control Parameters*. These Parameters, provided by any of the System Information Messages 1,2,2bis,3,4 and 9 also determine the authorized classes and authorized special classes in case of a non-emergency call.

The *RACH Control Parameters* element is coded as shown in Figure 2.7. AC 0...9 and 11...15 correspond to the access classes mobile systems can belong to. For a mobile station of access class N (and eventually $N_{special}$) access is not barred if at least one of the corresponding AC bits are coded with a '0'. The EC field (octet three bit three) concerns emergency calls. If it is set to '0' emergency calls are allowed to all mobile systems in the cell. If it is set to '1' emergency calls are only allowed to mobile systems that belong to a special access class.[04.08 '98], 3.3, 9.1, 10.5

8	7	6	5	4	3	2	1	
	RACH Control Parameters IEI							octet 1
Max retrans		Tx-integer				CELL BARR ACCESS	RE	octet 2
AC C15	AC C14	AC C13	AC C12	AC C11	EC C10	AC C09	AC C08	octet 3
AC C07	AC C06	AC C05	AC C04	AC C03	AC C02	AC C01	AC C00	octet 4

Figure 2.7: The RACH Control Parameter Information Element.

2.3.4 The Paging Channel

If a mobile is called, this call will be announced by the network by sending a paging (PAGING REQUEST) message on the PCH, the paging channel of the CCCH. This message will trigger the mobile to establish a RR connection and to receive the call. The mobile will subsequently send a CHANNEL REQUEST on the RACH indicating in the establishment cause field of this message that it has received a paging message. This causes the network to allocate a dedicated channel for this MS which will then send a paging response on the DCCH to the network. After the usual authentication process any data transmitted on this channel will be ciphered. [Lagrange '99] In a sequencing step the actual call establishment will be initiated by the network . See figure 2.8.

There are three different types of PAGING REQUEST as described in detail in table 2.3. Each request message contains 23 bits, which will be inflated by the correction code corresponding to the algorithm given in section 2.4.2. The resulting 116 bits are then sent on a normal burst as shown in figure 2.1.

- PAGING REQUEST type 1,
- PAGING REQUEST type 2,
- PAGING REQUEST type 3.

Information Element	length in octets for a PR type 1	length in octets for a PR type 2	length in octets for a PR type 3
L2 Pseudo Length	1	1	1
Protocol Discriminator	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
Skip Indicator	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
Message Type(type 1,2,or 3)	1	1	1
Page Mode	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
Channels needed for Mobiles 1 and 2	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
Mobile Identity 1	2-9	4	4
Mobile Identity 2	3-10	4	4
Mobile Identity 3		3-10	4
Mobile Identity 4			4
P1, P2, or P3 Rest Octets	0-17	1-11	3

Table 2.3: PAGING REQUEST type 1, 2 and 3 messages content.

The Information Elements contain the following information.

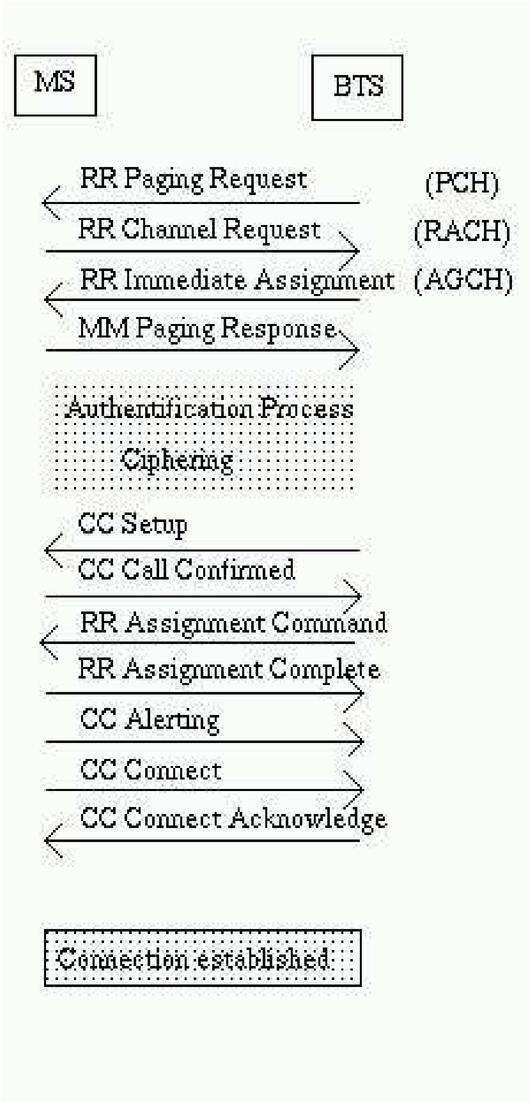

Figure 2.8: Messages triggered by a PAGING REQUEST message.

- The *L2 Pseudo Length* Information Element indicates the total length in octets of the PAGING REQUEST message. The L2 Pseudo Length Information Element itself is described in [04.08 '98] 10.5.2.19 .

- The *Protocol Discriminator* Information Element consists of four bits giving the protocol to which the message belongs. Here these bits are set to "0110", which stands for "radio resource management messages". It is defined in [04.08 '98] 10.2.

- If the *Skip Indicator* Information Element is set to "0000" the message shall be ignored.[04.08 '98] 10.3.1
- The *Message Type* Information Element is set to

  00100001 if it is a PAGING REQUEST TYPE 1 message,

  00100010 for a PAGING REQUEST TYPE 2 message,

  00100100 for a PAGING REQUEST TYPE 3 message.

  Further information about this Information Element can be found at [04.08 '98] 10.4.
- The *Page Mode* message can contain additional requirements on mobiles belonging to the paging subgroup of the sub-channel the message has been sent on. The mobile takes into account the Page Mode message of any message sent on its sub-channel. Two bits in this element are reserved for the message and indicate the following:

  00 no additional requirements

  01 extended paging: receive and analyze next but one message on the PCH

  10 paging reorganization: receive all messages; next action will be described in the subsequent message

  11 same as before

  (For more detailed information see [04.08 '98] 10.5.2.26)

  The paging group is calculated as follows.

  PAGING_GROUP(0...N)=((IMSI mod 100) mod (BS_CC_CHANS $*$ N))

  where N represents the number of paging blocks available on the CCCH and BS_CC_CHANS is the number of control channels given in the BCCH [05.02 '99] 6.5.2.
- The *Channel Needed* Information Element indicates which kind of channel is to be requested in the channel request in response to this paging message. The channel types are coded as follows. [04.08 '98] 10.5.2.8

  00 any channel

  01 SDCCH

  10 TCH Full rate

  11 TCH Full or Half rate
- The *Mobile Identity* Information Element provides either TMSI or IMSI (if no valid TMSI is available), indicating also which of them is used. If the message is a type 1 message the given mobile identities can either be TMSI or IMSI but the message can in any case only include 2 identities. Message type 3 was designed to address to 2 or 3 mobiles but only the third one can be identified by its IMSI. Message type 3 offers the possibility to page to 4 mobiles at the same time all being addressed to using their TMSIs.

  The exact bit-structure of the element is given in [04.08 '98] 10.5.1.4.

- The *P1 Rest Octets* contains details about the status of the information, priority level and spare bits.

The paging message is broadcasted in the LA (explained in section 2.2.2) the MS in currently situated in.

2.3.5 The Random Access Control Channel

The CHANNEL REQUEST message is sent by a MS in idle mode to the cell it is camped on to demand a dedicated channel. The message content is shown in Figure 2.9. The field for the establishment cause has a variable length from three bits up to six, whereas the random reference fills the remaining bits to the next octet. The use of this random number is to enable the network to distinguish two access demands originating from two different mobiles at the same time on the same frequency.

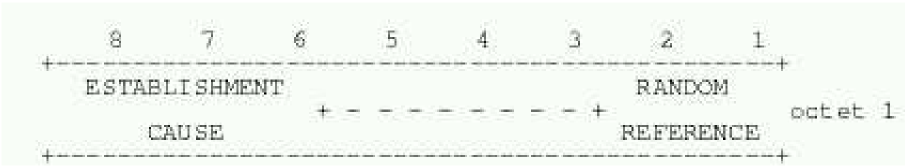

Figure 2.9: The CHANNEL REQUEST Information Element.

Table 2.4 represents an extract of the encoding of the establishment cause. The random reference digits are replaced by an "x". The complete coding table can be found at [04.08 '98] 9.1.8.

MS code bits 8 ... 1	establishment cause
101xxxxx	Emergency call
100xxxxx 0010xxxx 0011xxxx 0001xxxx	answer to paging (For more details see figure 2.10.)
000xxxxx 0000xxxx	Location updating
111xxxxx	originating call or text message
0100xxxx	originating speech call
0001xxxx	originating text message

Table 2.4: Establishment cause coding.

If the CHANNEL REQUEST message is sent in reply of a paging message the establishment cause will be coded as shown in figure 2.10.

MS Capability / Paging Indication	Full rate only	Dual rate	SDCCH only
Any channel	100xxxxx	100xxxxx	100xxxxx
SDCCH	0001xxxx	0001xxxx	0001xxxx
TCH/F	100xxxxx	0010xxxx	0001xxxx
TCH/H or TCH/F	100xxxxx	0011xxxx	0001xxxx

Figure 2.10: The CHANNEL REQUEST Information Element with establishment cause "answer to paging".

The CHANNEL REQUEST message is emitted on a single Access Burst (see figure 2.11 or 2.1) that transmits 156 bits emulated as described in [05.02 '99] 5.2.7. The encrypted bits (e0...e35) encipher the actual 8 bits describing the content of the CHANNEL REQUEST message. The accurate encryption algorithm is given in section 2.4.3

Bit number				
0.....7	8.....48	49.....84	85.87	88.....156
ext. tail bits	synchronization sequence bits (training bits)	encrypted bits	tail bits	extended guard period

Figure 2.11: Bit-Mapping on an Access Burst on the RACH.

2.3.6 The Access Grant Channel

The Access Grant Channel (AGCH) is a downlink channel used by the network to provide assignment information. After receipt of a CHANNEL REQUEST message sent by the MS on the RACH to demand a dedicated channel, the network tries to reserve either a SDCCH or a TCH for this MS. It subsequently sends an IMMEDIATE ASSIGNMENT (IA) message or an IMMEDIATE ASSIGNMENT EXTENDED (IAE) message containing information about the dedicated channel or an IMMEDIATE ASSIGNMENT REJECT (IAR) message to reject the channel demand. The message format is described in table 2.5.

The IA message contains assignment information for one mobile whereas the IAE message contains assignment information for two mobiles. The IAR message is sent if there is no channel available at that time. Any assignment message contains a random reference number that refers to the random reference sent in the CHANNEL REQUEST message that triggered the sending of the assignment message.

On receipt of an IA(E) message, corresponding to one of the last 3 CHANNEL REQUEST messages sent, the mobile stops sending more CHANNEL REQUESTS or stops the timer

T3126, that is started after sending the maximum number of CHANNEL REQUESTS allowed. The subsequent communication data will be sent on the dedicated channel given in the assignment message.

On receipt of an IAR message the mobile stops sending CHANNEL REQUESTS and starts the timer T3122, initiated with the time given in the rejection message (wait indication) and the timer T3126 (if not yet started).

The timer T3122 monitors the duration in which no new connection establishment attempts are allowed to be made except for emergency reasons. While the timer T3216 is running any other IAR received will be ignored. After expiration of this timer the mobile will return to CCCH idle mode, i.e. the immediate assignment procedure is aborted. If, on the other hand, an IA(E) message, corresponding to one of the last 3 CHANNEL REQUEST messages is received while the timer is still running the mobile will proceed as if there had never been a rejection message.

"As an option the mobile station may return to CCCH idle mode as soon as it has received responses from the network on all, or in case more than 3 were sent the last 3, of its CHANNEL REQUEST messages." [04.08 '98] 3.3.1.1.3

The 23 bits of the assignment messages are coded as described in section 2.4.2. The coded message is then sent to the network on a normal burst as shown in Figure 2.1.

The Information Elements contain the following information.

- *L2 Pseudo Length*: See section 2.3.4.
- *Protocol Discriminator*: See section 2.3.4.
- The *Message Type* Information Element is set to

  00111111 if it is an IMMEDIATE ASSIGNMENT message,

  00111001 for an IMMEDIATE ASSIGNMENT EXTENDED message,

  00111010 for an IMMEDIATE ASSIGNMENT REJECT message.

  Further information about this Information Element can be found at [04.08 '98] 10.4.
- *Page Mode*: See section 2.3.4.
- The *Spare Half Octet* fills to the next octet with zeros. [04.08 '98] 10.5.1.8
- The *Dedicated mode or TBF* IE is ignored by the mobile if it is not in GPRS mode. [04.08 '98] 10.5.2.25b
- The *Channel Description* Information Element gives information about the allocable channel together with its SACCH and is described in [04.08 '98] 10.5.2.5
- The *Packet Channel Description* IE is ignored by the mobile if it is not in GPRS mode. [04.08 '98] 10.5.2.25a

Information Element	length in octets for IAs	length in octets for IAEs	length in octets for IARs
L2 Pseudo Length	1	1	1
Protocol Discriminator (RR management)	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
Skip Indicator	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
Message Type (Immediate Assignment (Extended/Reject))	1	1	1
Page Mode	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
Spare Half Octet		$\frac{1}{2}$	$\frac{1}{2}$
Dedicated mode or TBF	$\frac{1}{2}$		
Channel Description (1)	3	3	
Packet Channel Description	3		
Request Reference (1)	3	3	3
Timing Advance (1)	1	1	
Wait Indication (1)			1
Channel Description (2)		3	
Request Reference (2)		3	3
Timing Advance (2)		1	
Wait Indication (2)			1
Request Reference (3)			3
Wait Indication (3)			1
Request Reference (4)			3
Wait Indication (4)			1
Mobile Allocation	1-9	1-5	
Starting Time	3	3	
IA Rest Octets	0-11	0-4	3

Table 2.5: IMMEDIATE ASSIGNMENT (EXTENDED) and IMMEDIATE ASSIGNMENT REJECT message content.

- The *Random Reference* refers to the random reference sent in the CHANNEL REQUEST message that triggered the sending of the assignment message. [04.08 '98] 10.5.2.30

- The *Timing Advance* IE is the binary representation of the timing advance in bits. 1bit $= \frac{48}{13}s$ [04.08 '98] 10.5.2.40

- The *Wait Indication* is used in the timer T3122 and provides the time the mobile has to wait before attempting the next channel request. [04.08 '98] 10.5.2.43
- The *Mobile Allocation* IE lists the frequencies of the cell allocation frequency list that have to be included in the mobile allocation frequency list. These lists provide the absolute radio frequency channel numbers (ARFCN) used in a frequency hopping sequence. [04.08 '98] 10.5.2.21
- The *Starting Time* IE gives the TDMA frame number (FN mod 42432) at which the mobile can start to use the given channel. [04.08 '98] 10.5.2.38
- The *IA Rest Octets* are basically spare parameters. The sum of this element and the L2 Pseudo Length IE must equal to 22. [04.08 '98] 10.5.2.16

[04.08 '98] 3.3.1.1.3 [04.08 '98] 11.1.2

2.4 Coding Schemes

The actual messages defined bit-by-bit in the Information Elements are coded as specified in the following sections. The purpose of error-correction codes is to protect the information bits against white noise (random noise) sources. A error-correction code inflates the initial amount of data a lot but allows the recipient to recover the original information even if there had been noise on e.g. the air interface between the mobile and the BTS.

Normal messages in GSM contain 184 data bits and pass through an error-correction process chain as shown in Figure 2.12 resulting in 8 blocks of 58 bits each. The stealing flag in step 3 contains 8 bits that are added to the 456 bits resulting from step 2. Along with each block there goes one stealing flag bit. For the channels BCCH, PCH and AGCH the stealing flag is dummy. The exact coding parameters are given in section 2.4.2. The 8 blocks of the final bits are sent on 4 normal bursts, sending 2 blocks on each burst.

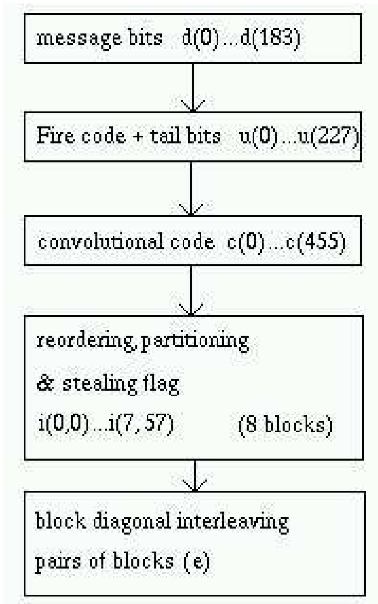

Figure 2.12: Channel coding for normal messages sent on f.e. the BBCH, the PCH or the AGCH.

Messages sent on the SCH or the RACH are treated differently and have their own coding chain as shown in Figure 2.13. SCH messages containing 24 data bits are inflated to 78 bits for the resulting correction code and RACH messages of only 8 bits result in a correction code of 36 bits. For details see sections 2.4.1 and 2.4.3. The 78 bits of the SCH message are sent on a single Synchronization Burst. The 36 bits of the CHANNEL REQUEST message are sent on one Access Burst.

Channel Coding for all GSM channel is described in [05.03 '99].

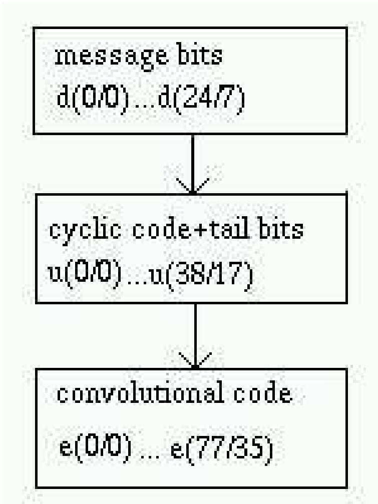

Figure 2.13: Channel coding for messages sent on the SCH or the RACH.

2.4.1 Coding Scheme for the SCH

The 78 bits (e(0) ...e(77)) in a Synchronization Burst emitted on the SCH channel that encrypt the actual 25-bit message (d(0) ...d(24)) are obtained as described below.

First 10 parity bits are added to the information bits. The parity bits are defined in such a way that

$$d(0)D^{34} + \ldots + d(24)D^{10} + p(0)D^9 + \ldots + p(9),$$

when divided by $D^{10} + D^8 + D^6 + D^5 + D^4 + D^2 + 1$ yields a remainder equal to $D^9 + D^8 + D^7 + D^5 + D^4 + D^3 + D^1 + D + 1$. Thus the encoded bits are:

u(k)= d(k) for k= 0,..., 24

u(k)= p(k-25) for k = 25, ..., 34

u(k)= 0 for k=35,..., 38 (tail bits)

The encrypted bits can then be obtained by the convolutional code using the polynomials

G0= 1+D^3+D^4

G1= 1+D+D^3+D^4.

resulting in

e(2k)= u(k) + u(k-3) + u(k-4)

e(2k+1)= u(k) + u(k-1) + u(k-3) + u(k-4)

for k=0,...,77 and u(k)=0 for k $<$ 0

2.4.2 Coding Scheme for BCCH, PCH and AGCH messages

The exact coding scheme used for normal messages is as follows. In a first step the 184 bits of information (= 23 Bytes) will be extended to 224 bits by a so called Fire code, a specific binary cyclic code. The generator polynomial is

G(D)=(D^{23}+1)$*$(D^{17} + D^3+1)

(for further information about Fire Codes see [Friedrichs '95]). This extension serves to provide error correction and detection. To these 224 (information and parity) bits another four bits equal to zero are added to fill the next byte. This block of 228 bits (u(0)...u(227)) is encoded with the $\frac{1}{2}$ rate convolutional code defined by the polynomials

G0= 1+D^3 + D^4 and

G1= 1+D+D^3 + D^4.

The result is 456 bits c(0)...c(455) defined by

c(2k)= u(k)+u(k-3)+u(k-4) and

c(2k+1)= u(k)+u(k-1)+u(k-3)+u(k-4).

The coded bits are reordered and interleaved according to the following rule:

i(B,j)= C(n,k) k= 0...455

n= 0,1,...N,N+1...

B= B_0+4n+(k mod 4)

j= 2((49k)mod 57)+((k mod 8) div 4)

The block of coded data is interleaved 'block rectangular', where a new data block starts every fourth block and is distributed over four blocks.

The interleaved bits are then mapped on bursts as follows.

$e(B, j) = i(B, j)$ and

$e(B, 59 + j) = i(B, 57 + j)$ forj= $0 \ldots 56$ and

e(B,57)= hl(B) and e(B,58)= hu(B).

hl(B) and hu(B) on burst number B are (stealing) flags used for indication of control channel signalling [05.03 '99] 4.1. The interleaving process is visualized in figure 2.14

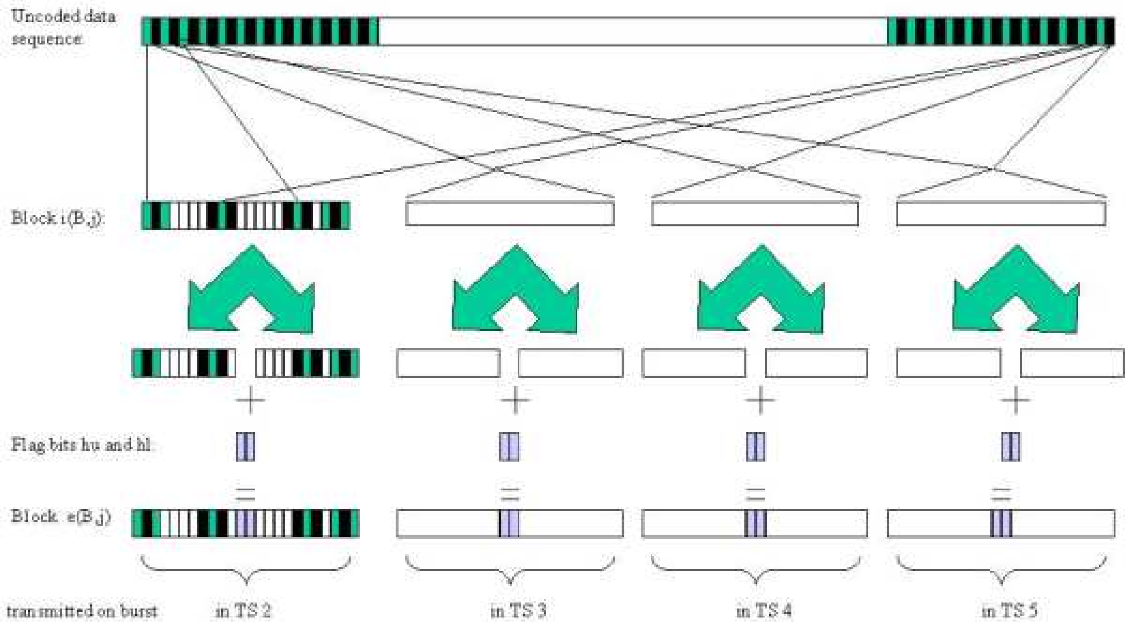

Figure 2.14: Visualization of the interleaving process.

The number of bits after coding hence comes up to 464. 464 bits can be transmitted on four normal bursts, 2∗58 bit each normal burst.

2.4.3 Coding Scheme for RACH messages

The 36 bits (e(0) . . . e(35)) in an Access Burst emitted on the RACH channel that encrypt the actual 8-bit message (d(0) . . . d(7)) are obtained as described below.

Six parity bits p(0) ... p(5) are defined in such a way that in GF(2) the binary polynomial

$$d(0)D^{13} + \ldots + d(7)D^6 + p(0)D^5 + \ldots + p(5),$$

when divided by $D^6 + D^5 + D^3 + D^2 + D + 1$ yields a remainder equal to $D^5 + D^4 + D^3 + D^2 + D + 1$. Furthermore 4 tail bits set to 0 are added and u(0)... (17) are defined as follows:

u(k)= d(k) for k= 0,..., 7

u(k)= p(k-8) for k= 8,..., 13

u(k)= 0 for for k= 14,..., 17

The encrypted bits e(0)... e(35) are then obtained by the convolutional code using the polynomials

G0= 1+D^3+D^4

G1= 1+D+D^3+D^4.

resulting in

e(2k)= u(k) + u(k-3) + u(k-4)

e(2k+1)= u(k) + u(k-1) + u(k-3) + u(k-4)

for k=0,...,17 and u(k)=0 for k $<$ 0.

Chapter 3

"Intelligent" concepts and possible hardware

3.1 Introduction to different concepts

Presented in this section are possible concepts for an intelligent cell phone silencer.

The main idea is as shown in figure 3.1. The cell phone silencer acts as a "man in the middle" between the BTS and all mobiles in the protected zone (cinema, theater, etc.). This means it either acts as the BTS with the biggest signal strength in the protected zone (for a chosen PLMN), taking over its "personality" i.e. making the MS believe it is the BTS itself (concept 1, 2 and 4) or vice versa it plays the role of the mobiles in the protected zone so the BTS only sees the mirrored MS signals (concept 3).

The black box has two separate antennas: one for signal reception and one for the emission of the modified signal. This is for two reasons. Firstly, the cell phone silencer has to listen to the incoming signal and emit its own at the same time. Secondly, the emitting antenna has to be separated from the receiving one since it otherwise would perturb its own incoming data.

Concept 1 The first idea is to change the access control data that is broadcasted by the BTS on the BCCH. The RACH Control Parameters (see section 2.3.3) indicate whether a mobile can use the cell it is camped on for normal services or for emergency calls only. If these parameters are set to "emergency service only" a mobile will not attempt to make or receive calls or text messages since it is convinced that its cell does not offer these services. The BCCH has to be emitted in the modified version constantly and with a significantly bigger signal strength than the BCCH version emitted by the BTS.

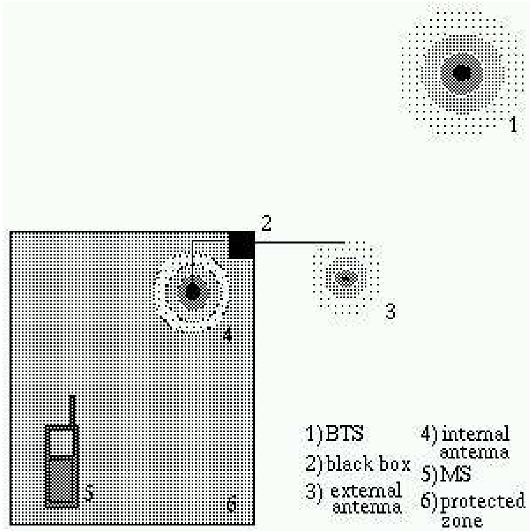

Figure 3.1: Scenario model.

In this case, the external antenna acts as the receiving antenna and the internal one as the emitting antenna.

Concept 2 This concept takes advantage of the paging control channel that informs a mobile in case of an incoming call (see section 2.3.4). The idea is to delete all paging messages and therefor hinder the mobile from making an attempt to receive a call in answering a paging message. Deleting messages means in this case simply perturbing the PCH constantly. Or the IMSI/TMSI of each message could be set to a non existent one.

Mobiles in the protected zone will still be able to make calls. They will only be prevented from receiving incoming calls or text messages.

As an option the Black Box could observe the PCH for paging messages for special numbers (IMSI, not phone numbers) and on receipt of such a number stop perturbing the channel for a moment and re-emit the message to the protected zone.

In this case, the external antenna acts as the receiving antenna and the internal one as the emitting antenna.

Concept 3 The third idea is to generally hinder the MS from requesting a dedicated channel on the RACH (see section 2.3.5). If all messages on the RACH except for those that ask for a dedicated channel to be able to make an emergency call, are deleted by the black box, the BTS will theoretically not notice that mobiles in the protected zone want to establish connections. Hence, there would be no possibility for a mobile in the protected zone to make or receive calls except for emergency calls. This concept implies that the direct connection between mobile and BTS would have to be cut which would in practice not be feasible .

In this case, the internal antenna acts as the receiving antenna and the external one as the emitting antenna.

Concept 4 The fourth concept is to spy on the CHANNEL REQUEST messages sent by the mobile. In case of a non-emergency request the phone silencer sends back immediately an IMMEDIATE ASSIGNMENT REJECT message for each CHANNEL REQUEST message observed. This has to be done before to mobile receives the IMMEDIATE ASSIGNMENT (EXTENDED) message sent by the BTS. As mentioned in section 2.3.5, there is an option that a mobile returns to idle mode if it receives an IAR on each of its channel requests. Since it is only a given option and not a definition of the GSM specification, it has to be determined (experimentally) whether this option is generally implemented or not, or if its implementation depends on the chosen network or on the terminal.

If the phone does not return directly to idle mode after receiving an IAR, it receives the IA(E) of the BTS too, which causes it to ignore the rejection message even if it was received first.

In this case, the external antenna acts as the receiving antenna and the internal one as the emitting antenna.

The most practical concepts seem to be concept one and two, since there seem to be no restrictions on their applications due to special network or mobile device features or technical obstacles.

To hinder cell phones from receiving calls, concept 2 could be applied, which would mean to constantly disturb the channel on which the network broadcasts message notifications (with some exceptions). To hamper a mobile system from both making and receiving calls (except emergency calls) concept 1 or 4 could work. Concept 1 implies constantly emitting a stronger system information signal, making the cell phone believe the system was in restraint service. Solutions 4 stands for the feigned rejection of call initiations but might not work for all phone types, since it is not mandatory for the MS (according to the GSM specification) to react on reception of an IMMEDIATE ASSIGNMENT REJECT [04.08 '98]. In any case an established connection will not be interrupted by the activation of the cell phone silencer device.

The possibilities a cell phone in the protected area has, depending on the concept used for the mobile blocker, are itemized in table 3.1.

Common to all practicable concepts (i.e. 1, 2, and 4) is the problem of perturbing the surrounding area of the protected zone, i.e.

- adjacent rooms
- by-passers

	receive calls	make calls	normal service for special groups	make emergency calls
concept 1	-	-	x	x
concept 2	-	x	x	x
concept 3	-	-	-	x
concept 4	-	-	-	x

Table 3.1: Functionalities of the four concepts.

as wave propagation is orbital, whereas rooms usually are rectangular (see figure 3.2). Perfectly shielding a hall the size of a cinema to keep waves from disturbing the normal network service outside is not feasible. The undesired effects though can be minimized, by optimizing the antenna's position and by adapting the cell phone silencer's signal strength to the size of the room and to the absorption capacity of the walls/the ceiling. Nevertheless, the silencer's operation time should be evaluated carefully.

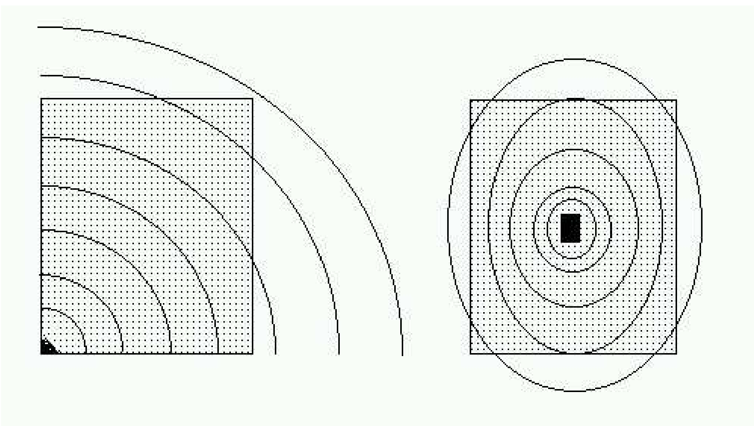

Figure 3.2: Problem of an exact covering of the concerned area for two types of antennas.

3.1.1 Functionalities

This section defines the functions to be implemented in the Black Box in order to realize the proposed concepts. The current supposition is that all these tasks only have to be executed for one single, fixed PLMN.

Common to all concepts are

- detection of the FCCH (frequency scan) and ability of frequency correction,
- detection and decoding of the SCH and ability to synchronize,

The realisation of Concept 1 also includes

- extraction and decoding of the BCCH of BTS with the biggest signal strength,
- the ability to extract and modify System Messages,
- the ability to re-emit the modified and re-coded versions.

Concept 2 requires

- extraction (and decoding) of the PCH,
- the ability to perturb the PCH,
- (the ability to forward certain PCH messages).

The implementation of Concept 3 needs

- detection and decoding of the RACH,
- the ability to delete certain channel request messages,
- the ability to isolate the RACH coming from the protected zone from the BTS.

The Concept 4 requires

- detection and decoding of the RACH,
- detection of the AGCH,
- the ability to create IAR messages and send them on the AGCH.

3.2 Operation status control

As already mentioned the phone silencer can as an unwanted side effect, also affect the surrounding area of the protected zone. Minimizing its operation time should therefor be one of the main goals. Presented below are several concepts of controlling the operation time. The first section will cover concepts that deal with the operation status control on behalf of the operator of the cell phone silencer. The second section will present two concepts for an external control of the device by the GSM service/network provider.

3.2.1 Owner controlled devices

There are several possibilities more or less dependent on human interaction to turn on or off a jammer device. At least one of them should be implemented in any case.

- Possibility to turn off power manually,
- addition of a user interface for programming operation times,
- observation of the channel RACH to detect mobiles in use,

  (If there have not been any messages on the RACH for a certain time the silencer could turn to standby mode, i.e. only listen to the RACH, until there are new messages and then return to normal mode.)
- observation of the RACH in a "learning phase" and later on use these results to estimate optimal operation periods,
- usage of an external monitoring system, e.g. infrared camera to observe human presence,
- usage of a static or mobile cell phone detector. Cell phone detectors react on send bursts of Location Updates of active cell phones in an adjustable action sphere.

3.2.2 Provider controlled devices

Besides control in behalf of the operator or a cognitive co-system it can also be thought of a possible intervention of the GSM network provider. The concept is hence to turn on and off the silencer via the air interface using normal GSM procedures.

With SIM card / provider contract Adding a SIM card maintained by the network operator to the silencer provides an easy way of controlling it by sending a text message, i.e. controlling it via the application layer.

Without SIM card / provider contract This concept allows the service provider to control the operation status of any phone silencer in its zone by broadcasting the control parameters on a normal control channel, just like System Information messages or paging messages. This concept hence works on the radio resource layer (layer 3).

3.3 Hardware solutions

The choice of the cell phone silencer hardware plays a very important role in the development phase and is therefor discussed separately.

Self-evidently, a cell phone silencer platform needs a Digital Baseband including a processor specialized on signal processing. It also has to integrate two antennas, one for the reception of the signal and one for the emission. Additionally, to connect the signal input and output to the signal processing part, an Analog Baseband needs to be added.

These components can be bought separately or already integrated on a complete platform. It can be thought of different scenarios / solutions (see figure 3.3).

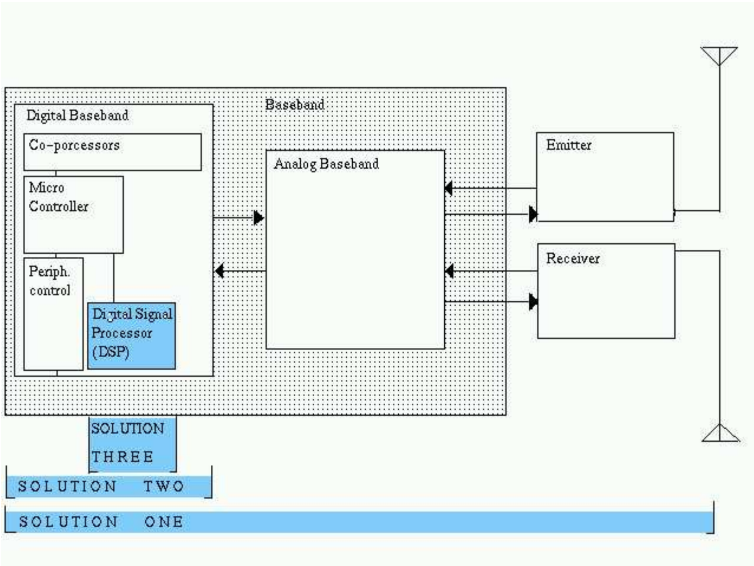

Figure 3.3: Block diagram for different chip design levels.

Solution One Starting from a complete platform, including all necessary components as the Digital Baseband Processor, the Analog Baseband, and the Receiver/Emitter.

Solution Two Taking the Digital Baseband and a suitable development environment to simulate the Analog Baseband and the Receiver/Emitter which are to be added separately to form a full platform .

Solution Three Choosing the Digital Signal Processor itself. This implies the complete process of chip development.

Advantages and Disadvantages of the three possible solutions

Solution One provides the least complicated way for an immediate start of the software development. It is certainly to be preferred if a platform can be found that corresponds to the block diagram 3.3 and provides open access to the channel layer. The problem is though, that such platforms are subject of a special sales strategy and not sold on the open market. Considering the projects time management, choosing Solution One results in a straight away start of the software development as it implies full hardware and software supply in behalf of the supplier. Apart from that costs are very easy to estimate since everything needed can be bought in the very beginning.

Solution Two implies the design of a card i.e. adding an Analog Baseband, an emitter and a receiver. Such a DSP usually comes with an development environment which can be used to start with the software development phase while designing the complete card in parallel. Solution Two is subject of the same sales strategy as Solution One. Costs too, can be estimated easily.

Solution Three really means to design the whole chip including, apart from an external Analog Baseband and the antennas, a micro controller and several peripheral controllers and co-processors. This solution allows to be totally independent of any supplier, but implies that a great time has to be used on the conception of the card, which also requires expert know-how in chip card design. Furthermore there is no existing set of functions preparing access to the channel layer. In total this implies a considerable delay to the begin of the actual software development which can not be started before the closure of the chip development phase. In addition there are no reliable sources about any cost estimations or time requirement.

Considering all of the possible big semiconductor suppliers, *Texas Instruments (TI)*, *Analog Device* and *Motorola* seem to have the most suiting components for designing a cell phone silencer platform. The different available devices and their categorization are shown in table 3.2. Their description and data sheets are given on the corresponding web pages [Instruments '02], [Device '02] and [Motorola '02].

	Solution 1	Solution 2	Solution 3	Description
Texas Instruments	TCS1100			mainly designed for GSM handset development
	TCS2100			provides advanced GSM (2.5) capabilities and GPRS functions
	TCS2500			most recent platform; GSM and GPRS funktions
		TBB1100		Digital Baseband of the TCS1100
		TBB2100		Digital Baseband of the TCS2100
		OMAP710		Digital Baseband of the TCS2500
			TBB1100	the Digital Baseband Processor used in the TCS1100
			TMS3200C6416	TMS320C64x DSP core + several coprocessors specialized for signal treating
Analog Device			ADSP_TS101S	optimized for telecommunication infrastructure applications; combines RISC, VLIW and standard DSP functionality
Motorola			DSP56305	DSP56300 + MCORE (MCU)
			DSP56654	DSP56600 + MCORE (MCU)

Table 3.2: Available platforms and DSP's.

Chapter 4

The SIMULATOR: Conception

Presented in the following sections are the concepts from those, that have been introduced in the previous sections. Section 4.1 details the concept chosen for the silencers functionality . Section 4.2 gives a new proposal for a provider-controlled operation status control system. Finally, section 4.3 states the suppositions the hardware has to fulfill and the most fitting platform.

4.1 The BCCH method

For the realization of the cell phone silencer simulator resulting from this report, the concept of changing the system information messages sent on the BCCH was chosen. It was chosen, mainly for its ability to hamper phones from both making calls (or sending sms') and receiving them. Furthermore this concept is independent from any special device or network feature and will hence work on any GSM cell phone in any GSM network. It will also be applicable to future devices. The main benefit this concept has, compared to the other three concepts proposed, is the feature of taking advantage of the 15 user classes every GSM mobile system belongs to. This allows a differential allocation of user rights according to the access class.

The disadvantage of this concept is that the BCCH has to be modified and re-emitted all the time. This means that a rather strong signal, that eventually also involuntarily disturbs adjacent areas, is emitted constantly. Compared to concept 4 which only triggers the cell phone silencer to send a contra-message when a channel request has been detected, the BCCH concept is not optimal in this objective. This disadvantage hence has to be compensated by a good operation status control strategy.

The functionality of the BCCH-method will hence be as follows. It firstly scans the frequency spectrum, looking for the strongest BTS and then synchronizes to this BTS. The strongest

BTS emission to the silencer will also be the strongest one to any mobile in the protected zone. The aim is to emit a stronger signal than the strongest BTS. Once synchronized to the BTS the silencer will take one 51-multitrame, extract the BCCH and change the RACH control parameters to the desired values. There is one System Information Message emitted every 0,235 s (every multitrame). This is the time that the device has to extract, change and recode the BCCH. The changed System Information Message will be re-emitted by replacing message "n+1" by the changed message "n". Messages that do not contain the RACH Control Parameters are simply forwarded. Though they, too, have to be extracted and decoded, to verify the type of the message.

4.2 The Notification Channel

The party that is hindering the cell phone silencers way to legality the most, is the network provider side. They obviously do not want anyone to be able to create zones in which their clients can not use the services. At least not without profiting from it.

The aim is, hence, to turn the provider side less adverse to mobile blockers. A way to get there can be to give them the possibility to act on the silencer, i.e. to control the silencers operation time and its capability characteristics.

A more elegant way to transfer the control information to the cell phone silencer than sending a text message, which includes that a SIM card had to be integrated into the silencer, is to let the BTS broadcast this information via the common downlink channels together with other system information.

The objective, by using the network services, is hence to find a free bit, or an equivalent, on the radio layer that can be used to inform a certain cell phone silencer to turn on/off the power including the classes which the silencer is allowed to hamper from.

This can be done by defining a new message type, using the radio resource management message type identifier 00100-011, which has been allocated but not used in previous phases of the RR protocol [04.08 '98].

This does mean a change to the GSM specification but would not have an disturbing effect on any other GSM device not implementing this feature, since unknown message types are simply ignored [04.08 '98] 8.4. The notification of a mobile phone silencer could hence be done by a message composed as shown in table 4.1.

The RACH Control Parameters allow the network operator to precisely define the classes that possibly can be hampered.

This newly defined message type can theoretically be sent on any common downlink channel, like for example the BCCH. It would not disturb other applications not sharing this new feature, since they will ignore it. It might though still be desirable to separate this message logically from other common system information to keep the clearness. Since there still is

Information Element	**Type/Reference**	**length in octets**
L2 pseudo length	L2 pseudo length [04.08 ’98] 10.5.2.19	1
RR management Protocol Discriminator	Protocol Discriminator [04.08 ’98] 10.2	$\frac{1}{2}$
Skip Indicator	Skip Indicator [04.08 ’98] 10.3.1	$\frac{1}{2}$
Silencer Notification Message (00100011)	Message Type [04.08 ’98] 10.4	1
RACH Control Parameters	RACH Control Parameters [04.08 ’98] 10.5.2.29	3

Table 4.1: Proposal of a cell phone silencer notification message.

an idle FN in TS 0 (see table 2.2), the notification message could be sent via this slot. If sent on the BCCH, Rest Octets would have to be added to make the total number of bits sum up to 23, which is the bit number entering the coding algorithm that codes a normal message sent on a normal burst (see figure 2.1). Rest octets do not carry any information and are filled with spare bits.

4.3 The OMAP710

Chronologically, the choice of the hardware for the silencer was the first objective of the project. The realization of a rather complex GSM application, as the one of a cell phone silencer based on modifying channels, needs a GSM base layer to work upon. The tasks of the layers one and two are not in the scope of this project. A potential platform hence has to come with an development environment that already includes the two lowest GSM layers but still provides access to layer 3 modifications.

Considering the solutions proposed in section 3.3, Solution 3 is therefor not practicable, since independency from a supplier also implies absence of any software support or GSM procedure library.

Solution 1 also does not apply to the projects needs, since the available platforms are constructed and specialized for either mobile systems or GSM base stations, which only have one antenna, that switches from emitting to receiving mode. A mobile blocker as proposed , however, needs two separate antennas to be able to listen to the BTS and remit the messages simultaneously. Thus remaining is Solution 2, i.e. a platform that still needs to be completed by adding a Analog Baseband and (in this case) two antennas.

A platform fulfilling these needs is the OMAP710 of Texas Instruments (see figure 4.1), a Digital Baseband and Application Processor. It is as according to TI broadly adopted in the marketplace for 2.5 and 3G wireless devices.

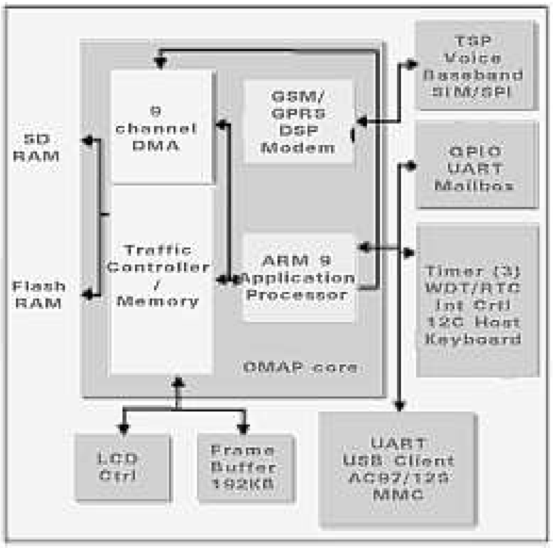

Figure 4.1: Blockdiagramm OMAP710.

It comes with the Code Composer Studio [Instruments '02], a development environment (C, C++, Assembler) for both ARM and DSP code generation. In a first step the OMAP710 platform will have to be completed by an external company by adding the Analog Baseband and the two Antennas. Then, another party has to piggyback layer 1 and 2 GSM functionalities on the platform. The resulting platform will be specialized to the projects demands in terms of both hardware and software requirements.

Chapter 5

The SIMULATOR: Implementation

Presented in the following sections are the concepts from those, that have been introduced in the previous sections. Section 4.1 details the concept chosen for the silencers functionality . Section 4.2 gives a new proposal for a provider-controlled operation status control system. Finally, section 4.3 states the suppositions the hardware has to fulfill and the most fitting platform.

5.1 User interface

The simulators user interface is as shown in screenshot 5.1.

The BTS can be triggered to emit messages on a common channel (i.e. write the corresponding data to a file) by clicking on the corresponding radio button.

The simulator emulates two kinds of mobile phones that evaluate the BCCH broadcasted by the BTS:

- one of the class 1...10,
- one of class 11...15, the so called VIP phones, held by the operator itself or emergency physicians.

Each type of mobile phone can be activated by the corresponding radio button. Their service state ("NORMAL SERVICE", "NO SERVICE", "EMERGENCY SERVICE ONLY"), that

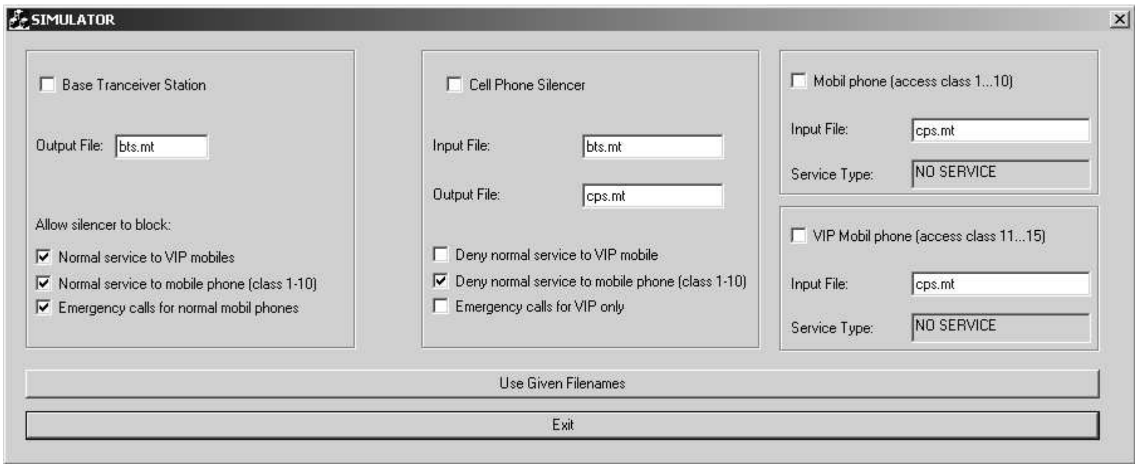

Figure 5.1: The simulator user interface.

is indicated in the non-editable field below, will change from NO SERVICE to NORMAL SERVICE, if both mobile phone and BTS are activated.

The cell phone silencer check button initiates the mobile jammer to change the RACH control parameters broadcasted by the BTS according to the values given in the check buttons in the lower part of the cell phone silencer field. Consequently mobile phones will change their service states, according to their type (normal or VIP) and the new RACH control parameters they receive. The change of service type could have a bit of a delay, since a mobile phone does not notice the change before the submittance of the next System Information Message that actually contains RACH control parameters (reminder: not all of them do).

This scenario can now still be influenced by the BTS by restraining the impact of the cell phone silencer, making use of the Notification Channel (FN 50 in TS 0). This can be done by clicking the desired check buttons in the lower part of the BTS field. Now the mobile phone cannot be hindered by the silencer. Even if the mobile jammer operator wished to do so, the values broadcasted by the BTS on the Notification Channel force the cell phone silencer to adjust its RACH control parameters.

The edit fields that are labelled "input file" and "output file" indicate the files to which the transmission data is written to and read from. Normally the input file of the cell phone silencer would be the output file of the BTS and the data written to the output file logically be the input to the mobile phone, but it can be thought of as different scenarios, as explained in section 6.1. The new filenames will be applied by clicking on the "Use new Filenames" button.

An example is given in screenshot 5.2.

The RACH Control Parameters (check button "Deny normal service to mobile phone (class 1...10")) set by the cell phone silencer force the normal mobile phone (check button "Mobile

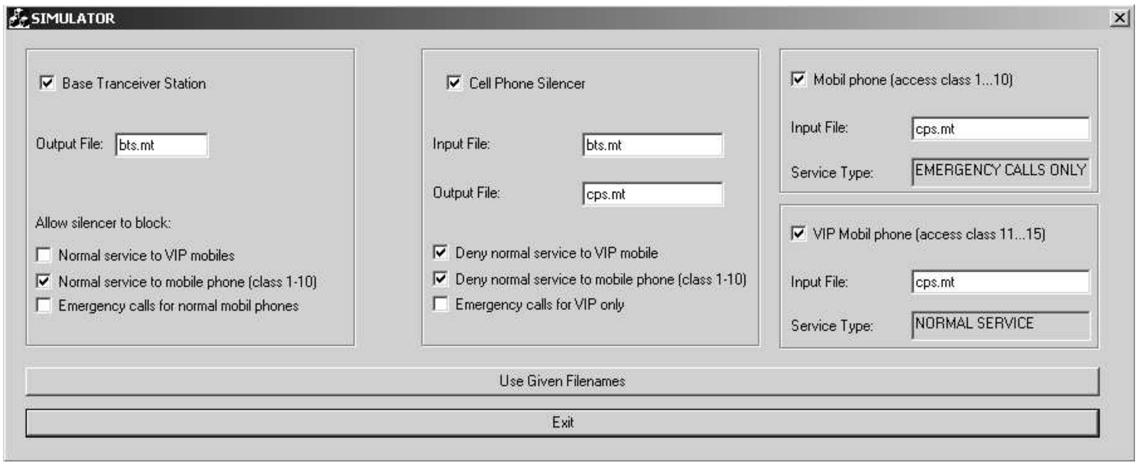

Figure 5.2: An example scenario.

phone (access class 1...10)") to switch to EMERGENCY CALLS ONLY. The VIP mobile phone (check button "VIP Mobile phone (access class 11...15)") though, is still in NORMAL SERVICE, even though, the jammer's check button "Deny normal service to VIP phones" is checked. This is because the BTS' "(Allow silencer to block ...) normal service to VIP mobiles" is not checked, which implicates that the silencer is not allowed to disturb the VIP phones service.

5.2 Component modelling

Presented in this section are the different components of the simulator.

Generally spoken, the components can be divided in five groups.

- Firstly there are the active components: the BTS, the cell phone silencer itself, and the mobile phone. All three of them are presented by a separate thread as shown in figure 5.3. They all inherit from CThread, which already defines the functions to change the filenames for in and output data.

  The *CGenerationThread* creates via GenerateMessage() a Multitrame that is then written to the output file. SetBlockRACH(...) proposes an interface to change the RACH Control Parameters (that are "blocked") on the Notification Channel. SetBSIC(...) changes the BSIC of the BTS, broadcasted on the SCH.

  The *CListenerThread* represents the cell phone silencer and re-emits (RemitMessage()) the data received by the BTS, with modified RACH Control Parameters (ChangeRACHSontrolParameters(...)) when activated (Power(...));

The *CMobilThread*, when activated, listens to the data (ListenToBCCH()) transmitted by the CListenerThread on the readfile and writes its service state to statusWnd according to the accessClass it has been constructed with.

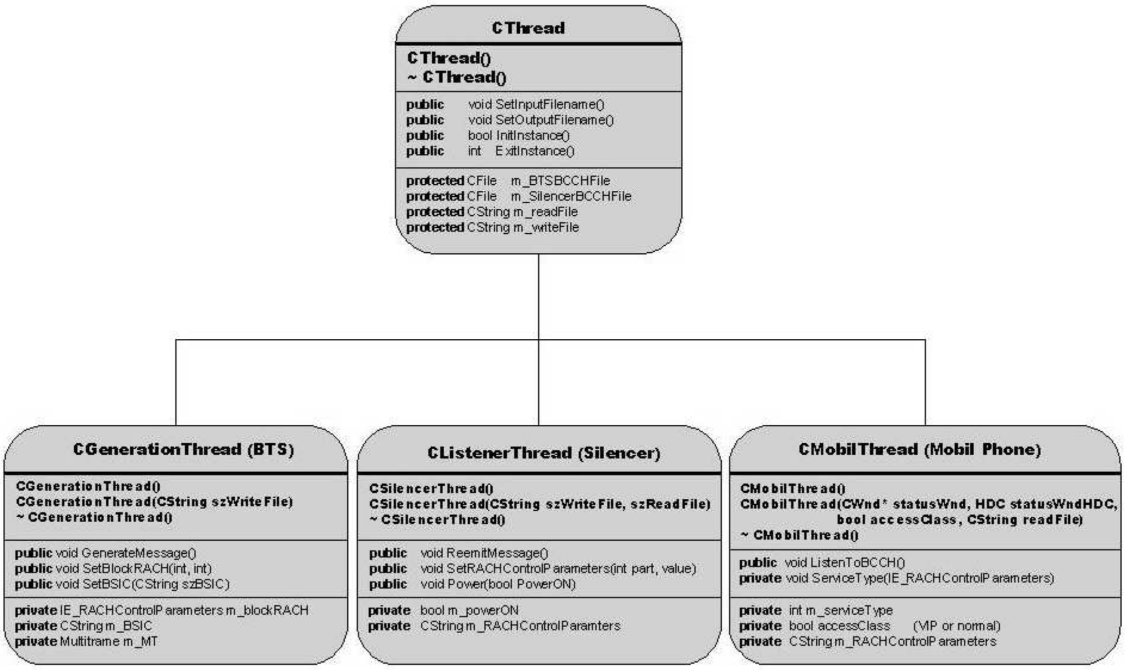

Figure 5.3: Component modelling of the Threads for BTS, cell phone silencer, and mobile phones.

- The *Multitrame* class represents the combination of all the channels that are really filled with data (the FCCH, BCCH, SCH and the Notification Channel) and all other channels, that are simply represented by a sequence of zeros in the Multitrames bit representation. The Multitrame can be constructed by the cell phone silencer's thread, by passing it the character sequence received by the BTS or by the BTS' thread, initializing it with the correct parameters.

- Thirdly there is the group of the component *"channel"*, such as the *FCCH*, the *BCCH*, the *SCH* and the *Notification Channel*. They all inherit the Function GetBitrepresentation(bool) off the general BCH_channel, which returns either the uncoded message or the final burst. All but the FCH, which is used only to be set by the BTS, have two constructors. The first one used by the CListenerThread: creates a new channel, by passing it the bits received by the BTS. The second one used by the CGenerationThread: creates a real new channel with the given parameters. Besides these, the important features transmitted on these channels can be easily accessed. For the SCH, these are the BSIC and the FN, for the BCCH it is the type of the system information message, that is broadcast and the RACH Control Parameters, that need to be

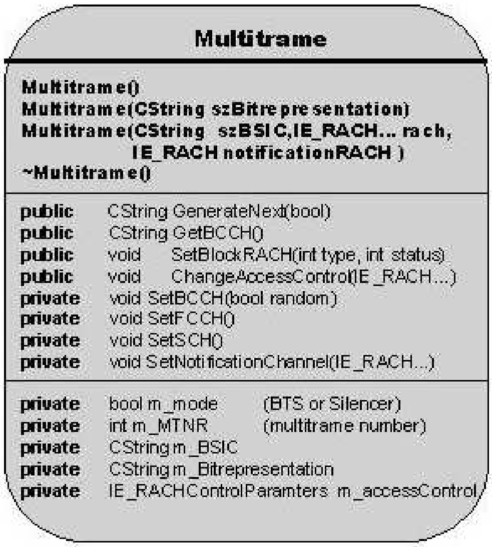

Figure 5.4: Component modelling for the Multitrame.

modifiable by the CListenerThread. The Notification Channel is only initialized once with the desired parameters by the BTS and is not meant to be changed by the cell phone silencer.

- Furthermore there is the group of the *radio resources messages*. They consist of the appropriate Information Elements. In figure 5.6 *System Information Message 1* and *System Information Message 2* are representatives of their type of messages. Type 1 has the Information Element RACH Control Parameters, like the types 2bis, 4 and 9. Type 2, 2ter, 3, 5, 6, 7, 8, 13, 16 and 17 do not. Type 1 offers a procedure to the Silencer to modify these parameters. So does the Notification Message that holds the RACH Control Parameters configuration that the BTS allows the cell phone silencer to modify.

- The last group of components are the Information Elements. Only two of these are implemented. Since the others are not connected to the accessControl checking, they are not modelled explicitly. They can be constructed, using the base class constructor InformationElement(int length), that simply creates an appropriate sequence of zeros. The RACH Control Parameters can be changed to grant or deny service access to the according access classes.

5.3 Collaboration diagram

This section visualizes the communication between the SIMULATOR's components triggered by a user interaction.

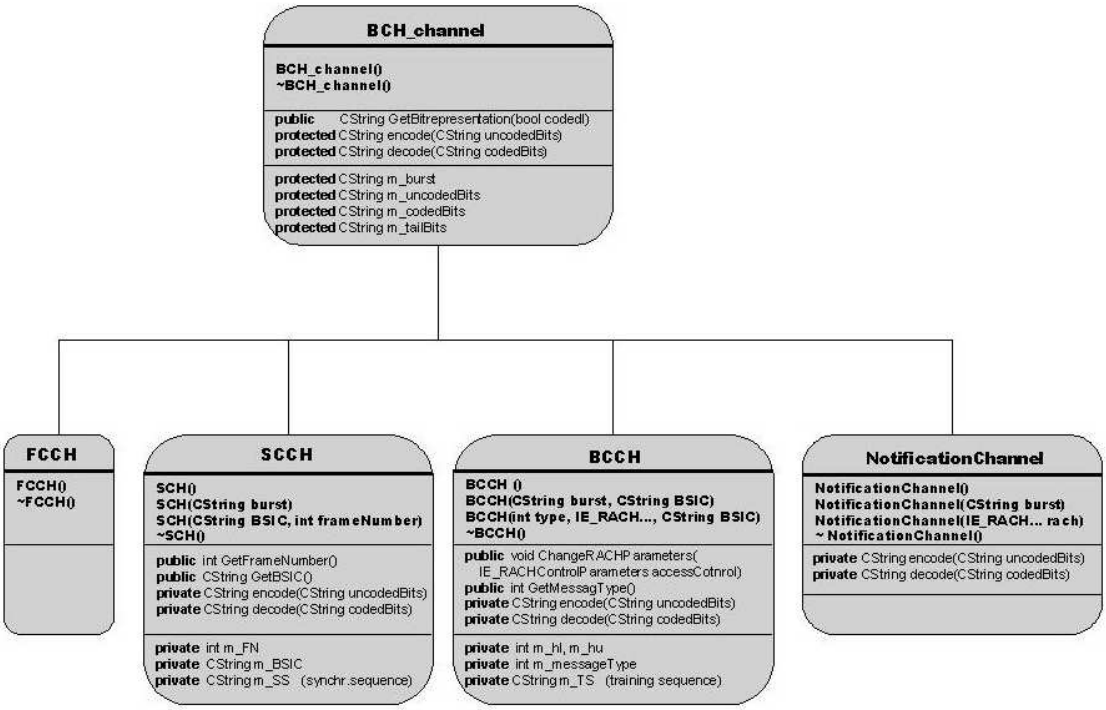

Figure 5.5: Component modelling for the Channels FCH, BCCH, SCH and the Notification Channel in FN 50 of TS0.

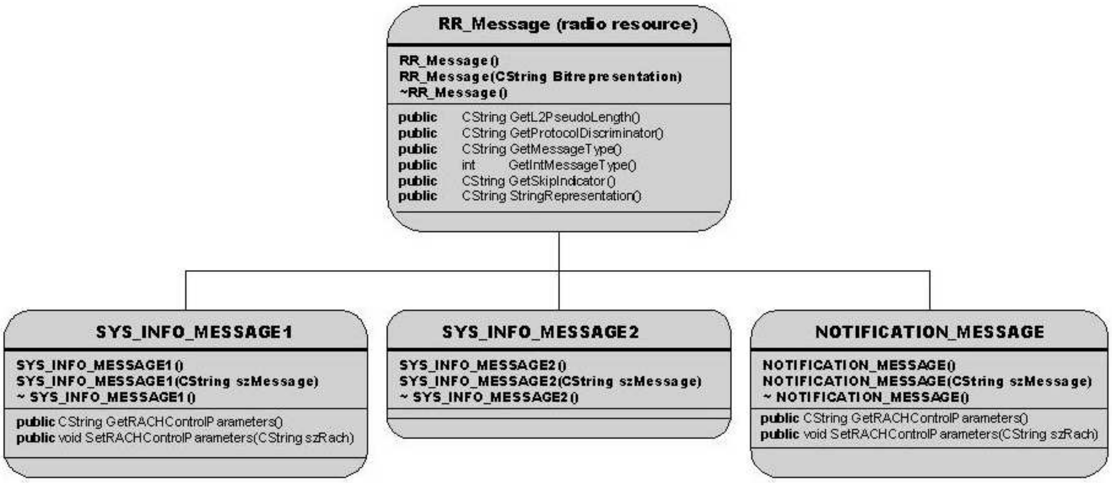

Figure 5.6: Component modelling of Messages sent on the BCCH and the Notification Channel.

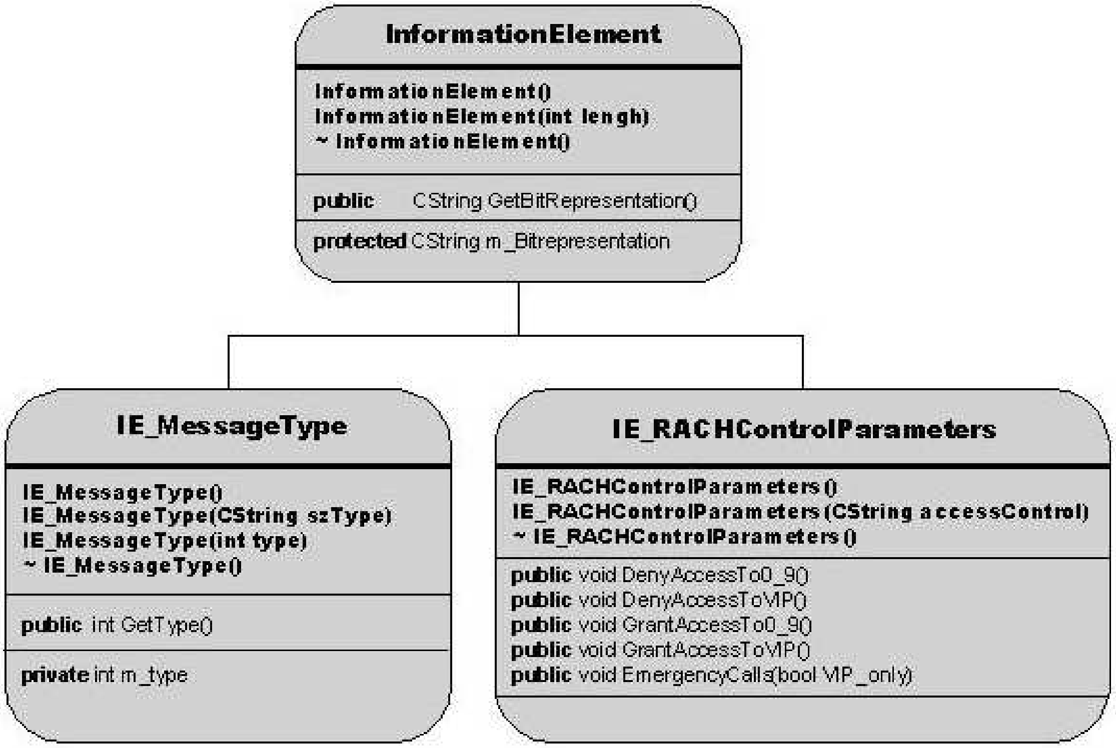

Figure 5.7: Component modelling of some Information Elements used in GSM RR Messages.

When the BTS is ticked, the dialog sends a message to the GenerationThread, that, if in resumed states, is reactivated and restarts to send messages (see figure 5.8).

The silencer's thread runs all the time and re-emits the messages received by the BTS' thread. If activated by the user, the ListenerThread starts modifying the BCCH of the received sequences as shown in figure 5.9.

On activation by the user, the cell phone's thread starts to read the data the silencer is emitting or forwarding, and to evaluate the RACH Control Parameters according to figure 5.10. Clicking on the control parameters in the lower part of the silencer and the BTS field modifies the RACH Control Parameters of the ListenerThread and the Notification Channel paramters of the BTS (see figures 5.11 and 5.12).

The filenames typed to the corresponding fields of the user interface are submitted to the particular threads, on pressing if the "use given filenames" button. The subsequent component interaction is as described in figure 5.13.

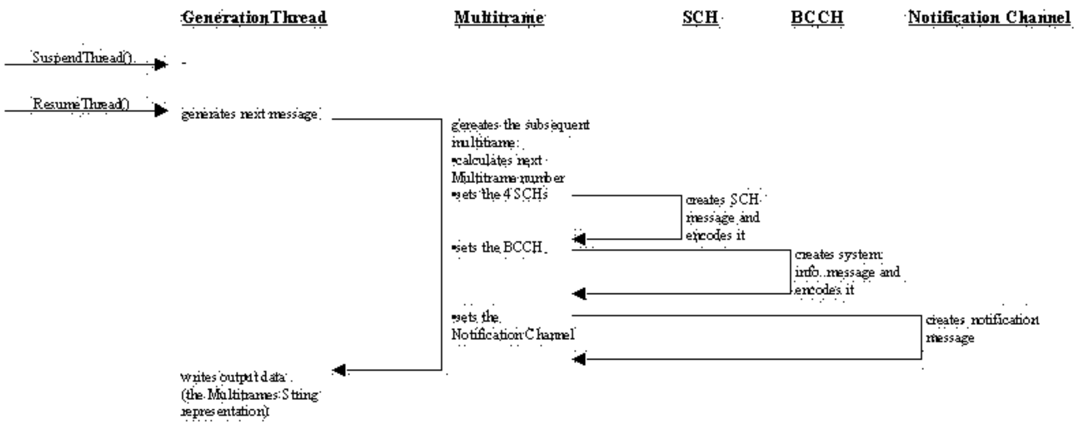

Figure 5.8: Communication triggered on pressing of the BTS button.

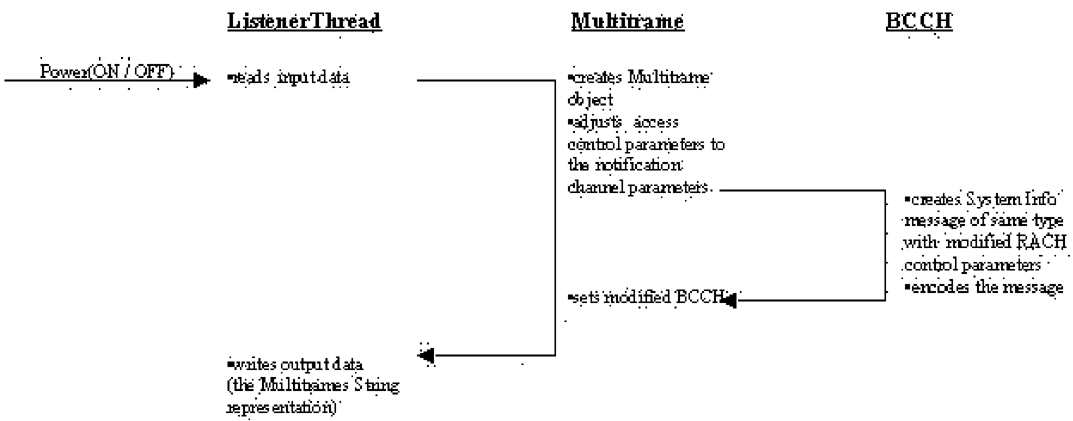

Figure 5.9: Communication triggered on pressing of the cell phone silencer button.

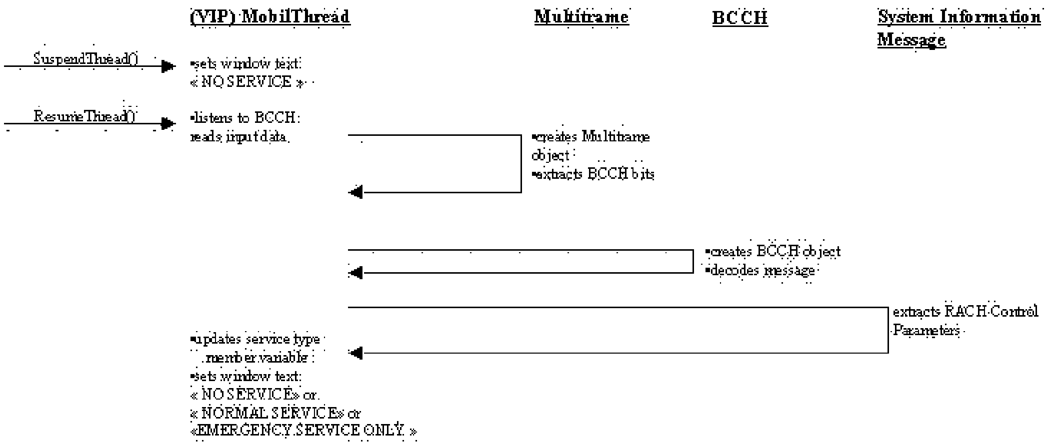

Figure 5.10: Communication triggered on pressing of one of the mobile phone buttons.

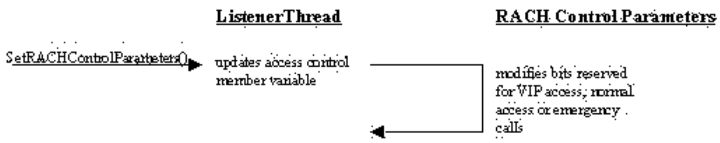

Figure 5.11: Communication triggered on pressing of one of the silencer's parameter buttons.

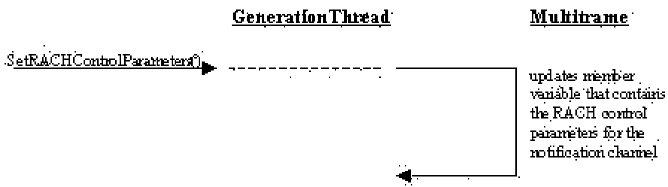

Figure 5.12: Communication triggered on pressing one of the BTS's paramter buttons.

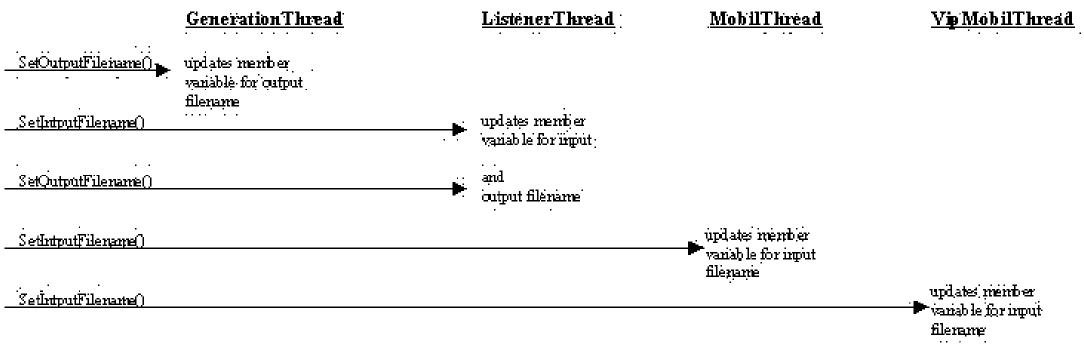

Figure 5.13: Communication triggered on pressing of the filename button.

Chapter 6

Integration in related projects

Starting from the idea of developing an intelligent cell phone silencer for GSM mobile phones, based on the BCCH concept, several tasks have arisen. The first one was object to this report: A feasibility study and development and comparison to other "intelligent" systems resulting in the implementation of a simulating system.

Two others shall be described in the following sections. Number one deals with the modulation and demodulation of the data circulating between the BTS, the mobile jammer and the mobile phone. The second one regards the usage of this kind of mobile jammer in cars in special view of the jammer's signal strength.

6.1 Simulation of the physical layer

To complete the simulator a second project was created that deals with the modulation of the data broadcast by the BTS and re-emitted by the cell phone silencer. It simulates the air interface using, according to the GSM, a GMSK modulation (Gaussion pre-filtered minimum shift keying). It interacts with the digital simulator as shown in figure 6.1. The BTS output data, that is written to the file, specified in the corresponding field of the user interface (see figure 5.1) is modulated and "transmitted" on the air interface. These waves then are demodulated and written to a new file, which filename has to be typed into the cell phone silencer input file field of the user interface. It then serves as input data to the mobile jammer simulator. The same procedure is applied on the output data of the jammer, that after modulation and demodulation serves as input data to the mobile phone.

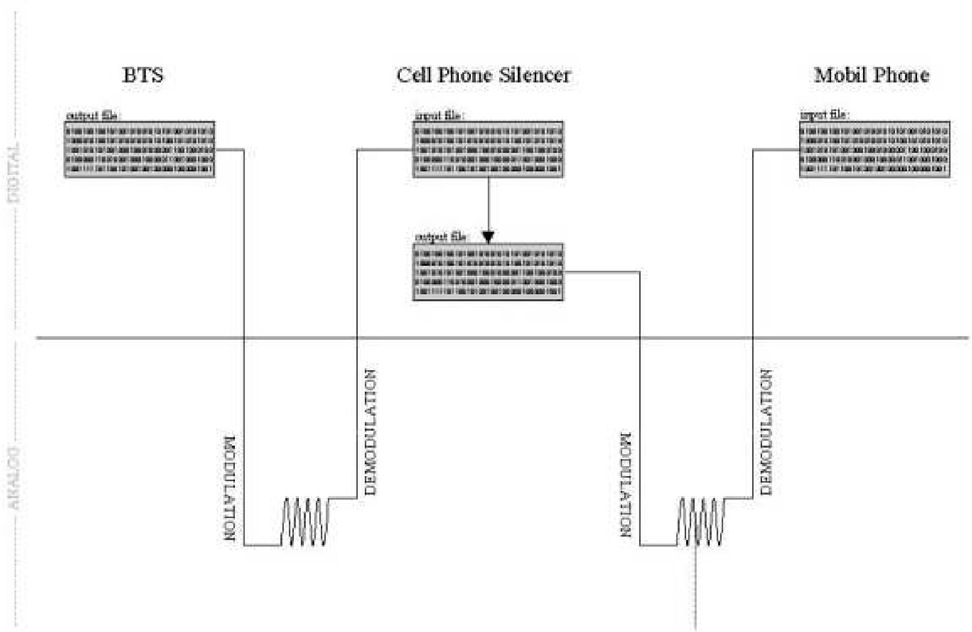

Figure 6.1: Interaction of the digital part (this project) and the analog part.

6.2 Optimal jamming level in cars

A possible application of the intelligent cell phone silencer could be its use in cars. If active, any inmate would be forced to use a hands-free-kit, that has its antenna outside the car. If there was no such a hands-free-kit in the car, the silencer would not modify the BTS signal. The aim is hence to create a minimal jamming zone, strong enough to keep the driver from using his mobile phone without the hands-free-kit.

The projects object is to measure the bacon channel inside a car while it is changing positions, in different environments, such as in the city, in the country etc. and find the optimal average signal strength for the cell phone silencer.

Chapter 7

Summary

In June 2002 negotiations between the ART (the French regulatory authority for telecommunications) [ART '02a], cell phone manufacturers, and potential cell phone silencer fabricators will start off a new phase in telecommunications. What has been forbidden so far, regarding the disturbing of reserved frequencies, will become legal for certain certified intelligent devices. Intelligent to the effect, that they block regular network service usage but let past emergency calls and communication of privileged cell phones.

The method of changing the access control parameters on the BCCH is one of the concepts that are likely to be legalized soon. The first object of this report was to develop other ideas for intelligent systems that are also based on the concept of the modification of common downlink channels and do work for any regular mobile phone, i.e. do not need additional features or technologies.

During the process of this report three such methods were developed, and compared to the BCCH model. Nevertheless, none of these new concepts matched with the BCCH idea. This is mainly because of the simple segregation of the cell phone spectrum in VIP and in regular cell phones by their RACH Control Parameters which are exploited by the BCCH cell phone silencer to differentiate easily between different levels of communication interference. Another benefit of this method is that it will work for any GSM cellular phone and therefor not disturb any other GSM applications independent from the access class control phenomenon. Last, but not least, the BCCH concept is superior to all other described concepts since it hampers both the making and the reception of a call or a text message by an affected mobile phone.

In addition a range of possibilities to control the power-on-time of the cell phone silencer have been developed. They can be separated into two groups: one that leaves the control to the operator of the cell phone silencer, and one that passes it to the network provider. Out of the proposed ideas the method of broadcasting the level , up to which the cell phone silencer is allowed to interfere (being a method of the second type), has proved to be the most reasonable. This is mainly for two reasons.

The first one is to turn the party of the network providers towards the idea of legalizing the interference of their networks by handing them the control over the cell phone silencers. This control would allow the providers not only to dominate the time cell phone silencers can possibly disturb their frequencies, but also to offer a new service to their clients: privileged cell phones, that work even in places disturbed by a cell phone silencer.

The second one being the smooth integration of the power-on-time control into the radio resource management layer, by using dead space in the GSM multitrame, which keeps the cell phone silencer independent from additional technologies.

A further object to this report was to fix a object design model for such a cell phone silencer concept (BCCH and Power-on-Time Control via the RR management layer). According to this model a simulator was implemented that emulates the data broadcasted by a BTS, received and re-emitted by a cell phone silencer and evaluated by a mobile phone. This simulator though, can only serve for demonstration purposes since it is not real-time capable.

The last task was then to examine the market for suitable hardware components for a real-time capable device. Based on this study and taking the code of the simulator as a model, a silencer device could be developed on a real DSP, such as the OMAP 710 which has proved to be one of the most suitable platforms available in the marketplace today.

AGCH Access Grant Channel
ARFCH Absolute Radio Frequency Channel Numbers
BA BCCH Allocation
BCCH Broadcast Control Channel
BCH Broadcast Channel
BSIC Base Station Identity Code
BTS Base Transceiver Station
CBCH Cell Broadcast Channel
CCCH Common Control Channel
CM Communication Management
DCCH Dedicated Control Channel
FACCH Fast Association Control Channel
FB Frequency Burst
FCCH Frequency Correction Channel
FDMA Frequency Division Multiple Access
FN Frame Number
IA IMMEDIATE ASSIGNMENT
IAE IMMEDIATE ASSIGNMENT EXTENDED
IAR MMEDIATE ASSIGNMENT REJECT
IE Information Element
IEI Information Element Identifier
IMSI International Mobile Subscriber Indentity
L2 Layer 2
LA Location Area
LAI Location Area Identity
LI Length Indicator
MM Mobility Management
MS Mobile Station
PCH Paging Control Channel
PLMN Public Lands Mobile Network
RACH Random Access Channel
RF Radio Frequency
RR Radio Resource
SACCH Slow Associated Control Channel
SCH Synchronization Channel
SDCCH Stand-Alone Dedicated Control Channel
SIM Subscriber Identity Module

SMS Short Message Service

T3122 timer set during random access, after receipt of an IAR message

T3126 timer started on receipt of an IAR message or after sending the max. allowed number of CHANNEL REQUESTS.

TCH Traffic Channel

TCH/FS TCH/HS Traffic for coded speech

TDMA Time Division Multiple Access

TMSI Temporary Mobile Subscriber Indentity

TS Time Slot

All abbreviations used in GSM specifications are provided in [01.04 '99].

The Training Sequence Code (bit 61-86) for a GMSK modulated normal burst is defined in [05.02 '99] as follows. The training sequence used by a BTS is given by the BCC (the three least important bits of the BSIC), broadcast on the SCH.

0	(00100101110000100010010111
1	00101101110111100010110111
2	01000011101110100100001110
3	01000111101101000100011110
4	00011010111001000001101011
5	01001110101100000100111010
6	10100111110110001010011111
7	11101111000100101110111100)

Table 1: TSC

The Training Sequence Code (bit 42-105) for synchronisation burst is defined in [05.02 '99] as follows.

(1011100101100010000001000000111100101101010001010111011000011011)

The extended tail bits leading an access burts are specified as follows.

(00111010)

The synchronisation sequence bits, representing the bits 8-48 in an access burst are usually

(01001011011111111001100110101010001111000).

As an alternative TS1

(01010100111110001000011000101111001001101)

or TS2

(11101111001001110101011000001101101110111)

can be sent if stated explicitly (see [04.06 '99]).

Given in this section are the formats of the System Information Element messages[1] 1, 2, 2bis, 2ter, 3, 4, 7, 8, 9, 13, 16 and 17 used to broadcast system information on the BCCH.

IEI	Information element	Type / Reference	Presence	Format	length
	L2 pseudo length	L2 pseudo length 10.5.2.19	M	V	1
	RR management Protocol Discriminator	Protocol Discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	System Information Type 1 Message Type	Message Type 10.4	M	V	1
	Cell Channel Description	Cell Channel Description 10.5.2.1b	M	V	16
	RACH Control Parameter	RACH Control Parameters 10.5.2.29	M	V	3
	SI 1 Rest Octets	SI 1 Rest Octets 10.5.2.32	M	V	1

Figure 1: System Information type 1 message content.

[1]The presence requirement indication is coded with an M ("Mandatory") if the IE has to be included and its absence will trigger a "missing mandatory IE" error message. C stands for "Conditional" and the inclusion of the IE depends on protocol specified conditions and may provoke a "missing conditional IE" or "unexpected conditional IE" error in behalf of the receiver. The presence or absence of O ("Optional")-IEs may not provoke any error messages. The format indication field is set to V ("Value only") to indicate that no IEI presence is to be expected and no Length Indicator (LI) will be given.[04.07 '98]

IEI	Information element	Type / Reference	Presence	Format	length
	L2 Pseudo Length	L2 Pseudo Length 10.5.2.19	M	V	1
	RR management Protocol Discriminator	Protocol Discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	System Information Type 2 Message Type	Message Type 10.4	M	V	1
	BCCH Frequency List	Neighbour Cell Description 10.5.2.22	M	V	16
	NCC Permitted	NCC permitted 10.5.2.27	M	V	1
	RACH Control Parameter	RACH Control Parameters 10.5.2.29	M	V	3

Figure 2: System Information type 2 message content.

IEI	Information element	Type / Reference	Presence	Format	length
	L2 Pseudo Length	L2 Pseudo Length 10.5.2.19	M	V	1
	RR management Protocol Discriminator	Protocol Discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	System Information Type 2bis Message Type	Message Type 10.4	M	V	1
	Extended BCCH Frequency List	Neighbour Cell Description 10.5.2.22	M	V	16
	RACH Control Parameters	RACH Control Parameters 10.5.2.29	M	V	3
	SI 2bis Rest Octets	SI 2bis Rest Octets 10.5.2.33	M	V	1

Figure 3: System Information type 2bis message content.

IEI	Information element	Type / Reference	Presence	Format	length
	L2 Pseudo Length	L2 Pseudo Length 10.5.2.19	M	V	1
	RR management Protocol Discriminator	Protocol Discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	System Information Type 2ter Message Type	Message Type 10.4	M	V	1
	Extended BCCH Frequency List	Neighbour Cell Description 2 10.5.2.22a	M	V	16
	SI 2ter Rest Octets	SI 2ter Rest Octets 10.5.2.33a	M	V	4

Figure 4: System Information type 2ter message content.

IEI	Information element	Type / Reference	Presence	Format	length
	L2 Pseudo Length	L2 Pseudo Length 10.5.2.19	M	V	1
	RR management Protocol Discriminator	Protocol Discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	System Information Type 3 Message Type	Message Type 10.4	M	V	1
	Cell Identity	Cell Identity 10.5.1.1	M	V	2
	Location Area Identification	Location Area Identification 10.5.1.3	M	V	5
	Control Channel Description	Control Channel description 10.5.2.11	M	V	3
	Cell Options	Cell Options (BCCH) 10.5.2.3	M	V	1
	Cell Selection Parameters	Cell Selection Parameters 10.5.2.4	M	V	2
	RACH Control Parameters	RACH Control Parameters 10.5.2.29	M	V	3
	SI 3 Rest Octets	SI 3 Rest Octets 10.5.2.34	M	V	4

Figure 5: System Information type 3 message content.

IEI	Information element	Type / Reference	Presence	Format	length
	L2 Pseudo Length	L2 Pseudo Length 10.5.2.19	M	V	1
	RR management Protocol Discriminator	Protocol Discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	System Information Type 4 Message Type	Message Type 10.4	M	V	1
	Location Area Identification	Location Area Identification 10.5.1.3	M	V	5
	Cell Selection Parameters	Cell Selection Parameters 10.5.2.4	M	V	2
	RACH Control Parameters	RACH Control Parameters 10.5.2.29	M	V	3
64	CBCH Channel Description	Channel description 10.5.2.5	O	TV	4
72	CBCH Mobile Allocation	Mobile Allocation 10.5.2.21	C	TLV	3-6
	SI 4 Rest Octets	SI 4 Rest Octets 10.5.2.35	M	V	0-10

Figure 6: System Information type 4 message content.

IEI	Information element	Type / Reference	Presence	Format	length
	L2 pseudo length	L2 pseudo length 10.5.2.19	M	V	1
	RR management Protocol Discriminator	Protocol Discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	System Information Type 7 Message Type	Message Type 10.4	M	V	1
	SI 7 Rest Octets	SI 7 Rest Octets 10.5.2.36	M	V	20

Figure 7: System Information type 7 message content.

IEI	Information element	Type / Reference	Presence	Format	length
	L2 Pseudo Length	L2 Pseudo Length 10.5.2.19	M	V	1
	RR management Protocol Discriminator	Protocol Discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	System Information Type 8 Message Type	Message Type 10.4	M	V	1
	SI 8 Rest Octets	SI 8 Rest Octets 10.5.2.37	M	V	20

Figure 8: System Information type 8 message content.

IEI	Information element	Type / Reference	Presence	Format	length
	L2 pseudo length	L2 pseudo length 10.5.2.19	M	V	1
	RR management Protocol Discriminator	Protocol Discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	System Information Type 9 Message Type	Message Type 10.4	M	V	1
	RACH Control Parameter	RACH Control Parameters 10.5.2.29	M	V	3
	SI 9 Rest Octets	SI 9 Rest Octets 10.5.2.37a	M	V	17

Figure 9: System Information type 9 message content.

IEI	Information element	Type / Reference	Presence	Format	length
	L2 Pseudo Length	L2 Pseudo Length 10.5.2.19	M	V	1
	RR management Protocol Discriminator	Protocol Discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	System Information Type 13 Message Type	Message Type 10.4	M	V	1
	SI 13 Rest Octets	SI 13 Rest Octets 10.5.2.37b	M	V	20

Figure 10: System Information type 13 message content.

IEI	Information element	Type / Reference	Presence	Format	length
	L2 pseudo length	L2 pseudo length 10.5.2.19	M	V	1
	RR management Protocol Discriminator	Protocol Discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	System Information Type 16 Message Type	Message Type 10.4	M	V	1
	SI 16 Rest Octets	SI 16 Rest Octets 10.5.2.37e	M	V	20

Figure 11: System Information type 16 message content.

IEI	Information element	Type / Reference	Presence	Format	length
	L2 Pseudo Length	L2 Pseudo Length 10.5.2.19	M	V	1
	RR management Protocol Discriminator	Protocol Discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	System Information Type 17 Message Type	Message Type 10.4	M	V	1
	SI 17 Rest Octets	SI 17 Rest Octets 10.5.2.37f	M	V	20

Figure 12: System Information type 17 message content.

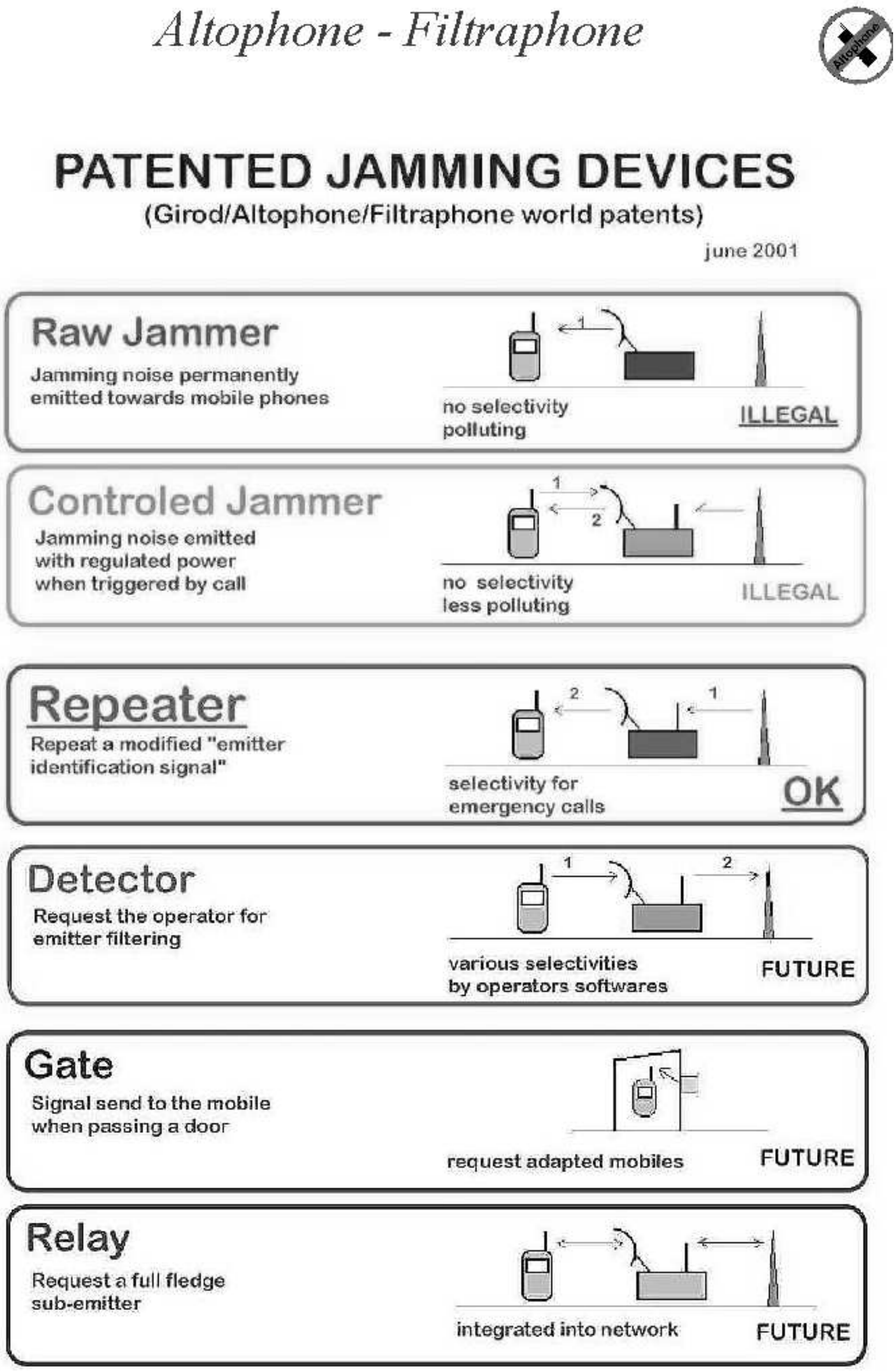

Figure 13: Patents of R. Girod.

Bibliography

[01.04 '99] GSM 01.04. Abbreviations and Acronyms (version 8.0.0 Release 1999) . http://www.etsi.org, 1999.

[03.22 '99] GSM 03.22. Functions related to Mobile Station in idle mode (version 8.5.0 Release 1998) . http://www.etsi.org, 1999.

[04.06 '99] GSM 04.06. Mobile Station-Base Station System Interface Data Link Layer Specification (version 8.1.1 Release 1999) . http://www.etsi.org, 1999.

[04.07 '98] GSM 04.07. Mobile radio interface signalling layer 3; General Aspects (version 7.3.0 Release 1998) . http://www.etsi.org, 1998.

[04.08 '98] GSM 04.08. Mobile radio interface; Layer 3 specification (version 7.9.1 Release 1998) . http://www.etsi.org, 1998.

[05.01 '99] GSM 05.01. Physical layer on the radio path; General description (version 8.6.0 Release 1999) . http://www.etsi.org, 1999.

[05.02 '99] GSM 05.02. Multiplexing and multiple access on the radio path (version 8.9.0 Release 1999) . http://www.etsi.org, 1999.

[05.03 '99] GSM 05.03. Channel coding (version 8.06 Release 1999) . http://www.etsi.org, 1999.

[05.04 '99] GSM 05.04. Modulation (version 8.1.2 Release 1999) . http://www.etsi.org, 1999.

[05.10 '99] GSM 05.10. Radio subsystem synchronization (version 8.8.0 Release 1999) . http://www.etsi.org, 1999.

[ART '01] ART. Les dispositions de la loi du 17 juillet 2001
. http://www.art-telecom.fr/textes/lois/index-01-624.htm, seen 12/01.

[ART '02a] ART. Autorite de Regulation des Telecommunications
. http://www.art-telecom.fr, seen O2/02.

[ART '02b] ART. Les differentes techniques
. http://www.art-telecom.fr/publications/index-brouille4.htm, seen O2/02.

[Bluelinx '02] Bluelinx. Q-Zone Courtesy System
. http://www.bluelinx.com/qzone.html, seen O2/02.

[Device '02] Analog Device. TigerSHARC DSP Products
. http://www.analog.com/technology/dsp/TigerSHARC/products.html, seen 01/02.

[Friedrichs '95] Bernd Friedrichs. *Kanalcodierung. Grundlagen und Anwendungen in modernen Kommunikationssystemen.* Springer Verlag, 1995.

[Girod '02] R. Girod. Patented jamming devices
. http://perso.wanadoo.fr/raoul.girod/page2.html, seen O2/02.

[Heine '98] Gunnar Heine. *GSM –Signalisierung verstehen und praktisch anwenden.* Franzis Verlag, 1998.

[Instruments '02] Texas Instruments. Wireless Chipset Solutions
. http://www.ti.com/sc/docs/apps/wireless/chipset/overview.htm, seen 01/02.

[Instruments '02] Texas Instruments. DSP Developers' Village
. http://dspvillage.ti.com/, seen O1/02.

[Lagrange '99] Xavier Lagrange. *Réseaux GSM-DCS.* HERMES Science Publications, Paris, 1999.

[Motorola '02] Motorola. Digital Signal Processors
. http://e-www.motorola.com/webapp/sps/site/taxonomy.jsp?nodeId=01M938562922795, seen 01/02.

[RegTP '02] RegTP. Die Regulierungsbehoerde fuer Telekommunikation und Post - Marktbeobachtung
. http://www.regtp.de/aktuelles/start/fs_03.html, seen O2/02.

Unité de recherche INRIA Rhône-Alpes
655, avenue de l'Europe - 38330 Montbonnot-St-Martin (France)

Unité de recherche INRIA Lorraine : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-0803